KU LEUVEN

FACULTY OF LAW AND CRIMINOLOGY

2023-2024

Cyber warfare: an attack on the principle of distinction?

A master's thesis on the emergence of a custom considering data an object under article 52(2) of Additional Protocol I to the Geneva Conventions

Promotor: Prof. dr. G. HERNÁNDEZ
Corrector: Prof. dr. B. KEIRSBILCK

Master's thesis submitted by
Charlotte TEUWENS

As part of the final examination for the degree of
MASTER OF LAW

KU LEUVEN

FACULTY OF LAW AND CRIMINOLOGY

2023-2024

Cyber warfare: an attack on the principle of distinction?

A master's thesis on the emergence of a custom considering data an object under article 52(2) of Additional Protocol I to the Geneva Conventions

Promotor: Prof. dr. G. HERNÁNDEZ
Corrector: Prof. dr. B. KEIRSBILCK

Master's thesis submitted by
Charlotte TEUWENS

As part of the final examination for the degree of
MASTER OF LAW

SAMENVATTING

Cyberaanvallen zijn alomtegenwoordig. De gevolgen ervan worden met de dag ernstiger. Deze aanvallen vereisen daarom een strenge en duidelijke regelgeving. Het merendeel van de staten besloot dan ook na jaren van discussie dat het internationaal humanitair recht van toepassing is op cyberoorlogvoering. Het blijft echter onduidelijk hoe de principes geïnterpreteerd moeten worden. Over het beginsel van onderscheid rees bijvoorbeeld de vraag of digitale gegevens als voorwerp beschouwd kunnen worden. In dat geval zou dit beginsel namelijk persoonsgegevens beschermen. Gezien de interconnectiviteit van de cyberruimte is dit dan ook zeer wenselijk.

In twee niet-bindende instructies over cyberoorlogvoering besloten experten daarentegen dat persoonsgegevens geen voorwerp zijn. Verschillende auteurs hebben kritiek geuit op deze interpretatie. Volgens hen beschouwen staten digitale gegevens reeds als voorwerp en ontstaat er gewoonterecht. In hun argumentatie voor deze verklaring ontbreekt echter sluitend bewijs.

Deze masterproef onderzoekt daarom de waarachtigheid van dit standpunt. De masterproef analyseert bronnenmateriaal van veertien staten op zoek naar *opinio juris* en statenpraktijk. De staten zijn geselecteerd aan de hand van drie factoren wat betreft hun betrokkenheid in cyberoorlogvoering. Op basis van deze analyse besluit de masterproef dat staten de ‘scale and effects approach’ toepassen: ze evalueren of de niet-materiële gevolgen van een cyberaanval, bijvoorbeeld economische, gelijkaardig zijn aan de gevolgen die een fysieke aanval zou veroorzaken. Het standpunt van de auteurs is dus gedeeltelijk waar: staten beschouwen digitale gegevens niet als voorwerp, maar wanneer de omvang en gevolgen van een cyberaanval een bepaalde drempel overschrijden, beschermen ze digitale gegevens alsnog als een voorwerp.

Deze bevinding resulteert in een alternatieve interpretatie voor huidige praktijken in de cyberruimte. Om vervolgens bovenvermelde drempel te specifiëren, zijn de interpretatie van de experten en de alternatieve interpretatie toegepast op scenario’s. Deze toepassing toont aan dat staten vaker bescherming bieden tegen cyberaanvallen dan de experten in hun interpretatie aan bescherming voorzien. De masterproef concludeert daarom dat een herinterpretatie wenselijk is om de rechtszekerheid en de bescherming van persoonsgegevens te verhogen.

ABSTRACT

Cyberattacks have become ubiquitous. The severity of their effects increases every day. They require a strict and clear regime. After thorough debate, a majority of the States hence decided that International Humanitarian Law applies to cyber warfare. The question remains, however, how the principles of this regime should be interpreted exactly in the light of cyberspace. For instance, regarding the principle of distinction, the question arose whether data is an object or not. If so, then civilian data would be protected under this cardinal principle, which is desirable due to the interconnectivity of cyberspace.

Two non-binding manuals presented by a group of experts nevertheless decided that this is not the case. Numerous scholars criticise the approach in these manuals for varying reasons. According to them, States are already considering data an object and, consequently, there is a custom emerging. They do not, however, present concise evidence for this statement.

As a result, this master's thesis investigates the truthfulness of this argument. In doing so, it looks at national sources of fourteen States, looking for evidence of both *opinio juris* and State practice. The States are selected using three factors relating to their involvement in cyber warfare. Based on this analysis, the thesis decides that States in general are using the scale and effects approach: they look whether the non-physical (e.g. economic) consequences are similar to the consequences a non-cyber operation would entail. The author's argument for criticising the manuals is therefore found half true: data is not considered an object. However, when the scale and effects of the attack reach a certain threshold, data is nevertheless protected as one.

This result presents an alternative interpretation for the current States' activities on cyber. To further determine the threshold for data to be protected as an object, the thesis links the findings of its research to scenarios. Both hypothetical and real-life examples of cyberattacks are analysed through the approach in the manuals and the scale and effects approach. It is shown that the approach taken by the States in their activities protects many more instances of intrusion than what the manuals currently uphold. The thesis concludes that the expected reexamination of the manuals is desirable to increase both the legal certainty around the topic and the protection of civilians' data.

ACKNOWLEDGMENTS

While writing this thesis, I have had the privilege of getting help from two groups of people. One group I know only from paper: they are the authors on whom this thesis is based. Their insights were enriching, their writing interesting and their conclusions provided me with plenty of 'food for thought'. However, it is the second group of people that will remain with me the most. The group that shaped this thesis from a to z, from blank line to comma, and from question to answer. They certainly deserve to be mentioned here.

I would like to start by thanking my promotor, professor Hernández. Thank you for giving me the opportunity to fulfil this research, for your valuable feedback, and your encouraging words. It was a joy to follow your courses and hear your insights.

Next, I want to thank my supervisor, Evelien Wauters. Thank you for reading my disorganised thoughts and your help to present them in a humanly readable structure. Your comments were incredibly useful and I am grateful for the valuable time you spend on our meetings.

I am also grateful for the advice of Karen Devos and Karel Brackeniers, who helped to bring shape to the original idea of the research and the methodology to complete it. In addition, I want to thank Justine Haekens for taking me on uplifting coffee breaks, answering all my questions, and giving me pep talks when I needed them. Having you as my 'buddy' during the research master truly was a great help these past two years.

Finally, I would like to thank my parents, my brothers, family, and friends. Thank you for your support, and especially your patience. The past five years included several stressful periods in which you all brought me comfort, each with your own *panacea*. From supportive comments to uncontrollable laughter, hugs, and tonnes of chocolate: I am lucky to have you as my personal pitcrew. And to my co-pilot, Andras, thank you for taking this road with me. I am excited to see where it leads us next.

CONTENTS

LIST OF ABBREVIATIONS

AP I	Additional Protocol I to the Geneva Conventions
CIL	Customary International Law
DCICIL	Draft Conclusions on the Identification of Customary International Law[1]
ICRC	International Committee of the Red Cross
IL	International Law
ILC	International Law Commission
ICJ	International Court of Justice
ICJ Statute	The Statute of the International Court of Justice
IHL	International humanitarian law
TM	Tallinn Manual
TM 2.0	Tallinn Manual 2.0
UN	United Nations
UN GGE	United Nations Group of Governmental Experts
UN OEWG	United Nations Open-ended Working Group
VCLT	Vienna Convention on the Law of Treaties

[1] International Law Commission, *Draft Conclusions on identification of customary international law, with commentaries* (2018).

LIST OF FIGURES

LIST OF ANNEXES

INTRODUCTION

1 *A viral topic* – 15 years ago, relatively little attention was given to cyberattacks.[2] Nevertheless, they occur against various governmental organisations, global businesses and even civilians' personal computers. This lack of attention has changed drastically over the past years. After having been the subject of numerous attacks, States and international organisations have realised the potential impact such operations can have. Given the interconnectivity of cyber networks, it is very unlikely for a cyberattack to limit itself to one victim or subject. Often, the actual attack takes place in one State, while the consequences are felt in a dozen. To that end, various (international) committees have outed their concern about this evolving method of infiltration and manipulation.

2 *Conferences* – To ensure cyber operations would not appear in a legal vacuum and sufficient cooperation is present, numerous conferences and working groups have been organised around this topic. With these initiatives, States have tried to tackle the questions this new type of attack raised. One of the most pivotal questions was: does international humanitarian law (hereafter: "IHL") apply? After years of debate, the consensus amongst States has arisen that IHL indeed applies. This consensus has been backed up by two reports: the Tallinn Manual and the Tallinn Manual 2.0 (hereafter: "TM and TM 2.0").

3 *Intent* – Even though the question whether IHL applies is resolved, the issue now concerns its exact application to cyber operations. Consequently, the master's thesis seeks common ground in the debate on one of the pivotal IHL principles: the principle of distinction. The thesis, however, goes further than the mere theoretical debate: it aims to put a scholarly argument into practice. Hereby, it analyses the current developments of States' activities on the topic. The goal is not to suggest any creation of new rules. Rather, the thesis assesses how the principle of distinction applies in modern day cyber operations when a common understanding by States on it is followed.

---

[2] The term 'cyberattack' and 'cyber operation' are used interchangeably in this thesis.

4 *Scenarios* – To present the findings of the States' activities analysis, the master's thesis uses five hypothetical scenarios, written by GEISS and LAHMANN.[3] These scenarios are supplemented by real-life cyber operations of which the lawfulness has remained contentious.[4] The real-life examples prove that the hypotheses are already part of today's reality. The scenarios are used to illustrate the scope and relevance of the issue, and thus of the research. They put the developed theory of how the principle of distinction should apply to cyberattacks, into practice. How do the findings of the master's thesis apply to each of the scenarios and, more specifically, the examples under consideration?

5 *Limitations* – In contrast with the previous paragraphs, it is equally important to address what the thesis does not do. First, it does not investigate the political motivations (for example: a link or a potential conflict with another State) behind a State's position: they are occasionally mentioned, but the thesis does not endorse an opinion as to whether that is truly the reason for a State's opinion. Although this could present interesting conclusions, it would lead too far from the main legal research. Second, relevant State documents published or adopted after 15th May 2024 were not included in the research of the State's activities because of the defined timeframe. Third, the research zooms in on a small aspect of a large debate on how cyber operations can be depicted in the light of IHL. It takes place in a much larger context of unresolved issues. The thesis will refer the reader to different aspects of these issues, which are justly interesting but will not be further developed.[5] Consequently, rather than solving the entire uncertainty regarding cyber warfare, the thesis is aimed to encourage scholars, legal practitioners, international institutions *et cetera* to continue with research on this problem.

6 *Format* – The thesis consists of two parts. The first part is theoretical, presenting a general overview of the context, the research questions, and state of the art. The second part consists of an analysis of State's activities on cyber warfare. It explores the argument that, regarding the principle of distinction, State practice and their beliefs are heading towards the emergence of a custom considering data an object.[6]

---

[3] See *infra* annex 1.
[4] See *infra* annex 1.
[5] For example, the question regarding how to interpret the notion of "attack" in cyberspace.
[6] Henning Lahmann, "State Behaviour in Cyberspace: Normative Development and Points of Contention," *Zeitschrift Für Außen- Und Sicherheitspolitik* 16, no. 1 (March 2023): 31-41; Paul B. Stephan, "Big Data and the

PART I: GENERAL INFORMATION ON CYBERATTACKS

CHAPTER I: THE CONTEXT AND THE RESEARCH QUESTIONS

7 *Roadmap* – The first chapter starts with an analysis of the gap in the literature around the principle of distinction which triggered the research question. Next, it provides some additional remarks, after which the actual research question will be explored. Furthermore, the chapter clarifies the relevance of the research about cyber operations and the status of data in IHL.

1. The Research Context[7]

§1. The issue: attacking civilians through their data

8 *Example* – In 2017, Russia was accused of a cyberattack against Ukraine, irreversibly corrupting databases containing essential digital data (hereafter: "data") of both civilian and governmental assets.[8] On the one hand, this resulted in a mere economic loss: the data was gone but the computers continued to function.[9] On the other hand, the operation led to a denial of service of a radiation monitoring system at Ukraine's Nuclear Power Plant.[10] A denial-of-service attack is an operation which does not cause physical damage directly but degrades the functioning of a system which results with ramifications in society.[11] In the example of Russia and Ukraine, the attack first resulted in consequences which only concerned cyberspace. Conversely, the consequences of the attack later entered the physical world. Following through, one could ask the following questions. Do both of these results constitute a violation of IHL?

Future Law of Armed Conflict in Cyberspace," SSRN Scholarly Paper, accessed March 20, 2024, https://papers.ssrn.com/abstract=3521387; Yunus Emre Gül, "Changing Notion of Object and Targeting Data Under the Law of Armed Conflict," *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi* 27, no. 2 (December 2021): 1298-1313.

[7] Based upon the Research Proposal by Charlotte Teuwens, 2023.

[8] "Notpetya (2017)," UN Cyber Toolkit, accessed March 20, 2024, https://cyberlaw.ccdcoe.org/wiki/NotPetya_(2017)#:~:text=The%20NotPetya%20malware%20was%20spread,and%20repurposed%20by%20the%20GRU.

[9] *Ibidem.*

[10] *Ibidem.*

[11] "Scenario 22: Cyber methods of warfare," UN Cyber Toolkit, accessed December 19, 2023, https://cyberlaw.ccdcoe.org/wiki/Scenario_22:_Cyber_methods_of_warfare.

Or is there a difference, depending on the nature of consequences? Is corrupting, encrypting, and destroying data similar to corrupting and destroying paper files or not? Is data an object? If so, then cyber operations against data are governed by the protective obligations relating to civilian objects, such as the principle of distinction, described in IHL.[12] If not, then many civilian datasets would be "fair game".[13]

9 *Increasing operations* – The previous paragraph gives an illustration of a cyber operation used as part of an armed conflict.[14] States and international organisations believe that their potential to easily target civilians by attacking their data *via* interconnected networks, raises increasing concerns.[15] Civilians have become the principal victims of these operations, which goes against all principles on armed conflicts.[16] Legally speaking, the most pressing issue is the lack of clarity on the types of operations which can be considered unlawful.[17] These considerations make it crucial to work towards a decent regulation.[18]

§2. A first and second attempt at clarification: the Tallinn Manuals

10 *Tallinn Manuals* – After years of various statements by State authorities and scholars discussing the issue, a majority opinion concluded that IHL is indeed applicable to cyber warfare.[19] This conclusion however, was not sufficient to fully solve the problem: the question merely shifted from whether to how IHL applies to cyber warfare.[20] In order to answer the latter, a group of experts, supported by an international organisation (the North Atlantic Treaty Organisation: NATO) and with extensive consultations with over fifty States, published two non-binding

---

[12] Kubo Mačák, "From the Vanishing Point Back to the Core: The Impact of the Development of the Cyber Law of War on General International Law," *9th International Conference on Cyber Conflict (CyCon)* (2017): 1-14.
[13] *Ibidem.*
[14] Stephan, "Big Data and the Future Law of Armed Conflict in Cyberspace". For other examples: see annex 1.
[15] *Ibidem.*
[16] Eve La Haye, *War crimes in internal armed conflicts*, (Cambridge: Cambridge University Press, 2008), 1 and 57.
[17] *Ibidem.*
[18] "ICRC Report 2020," ICRC, accessed March 20, 2024, https://www.icrc.org/en/document/annual-report-2020.
[19] Tatjana Grote, "Best of Both Worlds? The Interplay between International Human Rights Law and the Law of Armed Conflict in Cyberspace," *LSE Law Review*, no. 8 (2023): 179-226.
[20] Michael N. Schmitt, "Rule 80", in *Tallinn Manual 2.0 on the International Law applicable to cyber-operations prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence*; ed. Michael Schmitt (Cambridge: Cambridge University Press, 2017), 375; Aurel Sari, "Hybrid Threats and the Law: Concepts, Trends and Implications", *Hybrid CoE Trend Report*, no. 3 (April 2020): 1-28.

(Tallinn) manuals, explaining their conception of how IHL principles should apply to cyber operations.[21] These manuals are, due to the large variety of qualitative experts cooperating on the project and the rigorous process employed, considered a highly important resource for governments and legal advisors around the world.[22]

11 *TM versus TM 2.0* – Shortly after the first TM was published, the discussions restarted and a second manual was published in 2017. The reason is that the first TM focused specifically on IHL. However, understanding the difficulty of assessing whether a cyberattack rose to the level of an armed conflict, TM 2.0 also deals with cyber operations outside of an armed conflict, including issues of general State responsibility, extraterritorial jurisdiction, and specialised regimes such as international human rights law[23] Appropriately, TM 2.0 became a more extensive volume: it consists of four parts and only the fourth part deals with what already had been set out in the first TM, namely IHL.[24] Part I covers general IL, part II specialised regimes, and part III international peace and security in relation to cyber.[25] Important, these manuals are based in a logic of merely restating *lex lata*: unless consensus amongst all experts could be achieved, they did not try to push boundaries by positing any *de lege ferenda*.[26] As a result, only clarity is brought regarding the issues on which the experts could agree: the rules required consensus.[27] When there is no agreement on a question, the manual makes note of this process in the commentaries.[28] Consequently, the most controversial aspects are left out in the open in the manuals.

---

[21] Art. 52(2) Additional Protocol I (hereafter: "AP I").
[22] Schmitt, *Tallinn Manual 2.0*, xxii and xvi.
[23] Eric Talbot Jensen, "The Tallinn Manual 2.0: highlights and insights," *Georgetown Journal of International Law,* no. 48 (2017): 735.
[24] Jensen, "The Tallinn Manual 2.0," 740.
[25] *Ibidem.*
[26] The promotor of this master's thesis, professor Hernández, was part of the experts group and confirmed that this was the approach taken in the negotiations.
[27] Jensen, "The Tallinn Manual 2.0," 739.
[28] "Israel's cautious perspective on International Law in cyberspace: part II (jus ad bellum and jus in bello)," EJIL Talk: Blog of the European Journal Of International Law, accessed April 15, 2024, https://www.ejiltalk.org/israels-cautious-perspective-on-international-law-in-cyberspace-part-ii-jus-ad-bellum-and-jus-in-bello/.

12 *Armed conflict* – TM 2.0 starts by explaining that "*cyber operations executed in the context of an armed conflict are subject to IHL*".[29] There does not, however, exist in IHL any specific rule encompassing cyber operations. Consequently, the existing IHL principles must be interpreted in the light of a cyberattack instead of general kinetic warfare. A first obstacle for this is the minimum threshold of IHL: for it to apply, an armed conflict must exist.[30] The present master's thesis only considers cases in which this threshold is fulfilled, because then the IHL principles, among which the principle of distinction, fully apply.[31] For example, TM 2.0 confirms the threshold being fulfilled in the earlier mentioned example between Russia and Ukraine.[32] Following through in the application of IHL, then, one can start by looking into the various principles.

13 *Origin of attack* – Continuing its reasoning, the experts in TM 2.0 confirm that having complete conclusions on the origin of a cyberattack is not easy, which makes applying IHL difficult.[33] Indicating the true originator, finding out its true intents, and identifying a detailed overview of the effects is a challenge in cyberspace.[34] These factual difficulties should still not be an excuse to entirely prejudice its application: basic IHL principles such as the principle of distinction or the prohibition of unnecessary suffering apply regardless of the method of warfare employed.[35] But what are considered the 'basic principles of IHL'? TM 2.0 states that one of the most helpful tools for knowing the principles that apply to cyber warfare, is to look whether a principle is embodied in Additional Protocol I (hereafter: "AP I") of the Geneva Conventions.[36] Following that reasoning, the principle of distinction applies to cyber warfare, since article 51 and 52(1) AP I form the basis of the pivotal principle.[37]

---

[29] Schmitt, "Rule 80", 375-377.
[30] *Ibidem.*
[31] Schmitt, *Tallinn Manual 2.0*, 422. As earlier mentioned, there still exists a whole debate on if and when a cyberattack as such could fulfill the threshold of an armed conflict. This debate is not part of the research, since it takes place in cases where this threshold is assumed to be fulfilled. It chose to focus on the application of a principle of IHL itself, instead of on whether IHL applies or not to a certain scenario.
[32] Schmitt, *Tallinn Manual 2.0*, 376.
[33] Schmitt, *Tallinn Manual 2.0*, 377, 418 and 420.
[34] *Ibidem.*
[35] Schmitt, *Tallinn Manual 2.0*, 414.
[36] Schmitt, *Tallinn Manual 2.0*, 377.
[37] *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, ICJ Reports 1996, §78 (Nuclear Weapons case).

14 *Principle of distinction* – According to this particular principle, States should never use weaponry that cannot distinguish between civilians and combatants, as well as between civilian objects and military objectives.[38] That obligation includes cyber weaponry.[39] Rule 94 and 99 of TM 2.0 confirm respectively articles 51 and 52(1) AP I by explicitly prohibiting targeting the civilian population and their objects through a cyberattack.[40] In addition, since this principle is recognised as *jus cogens,* any justification of violating the principle is irrelevant for the conviction of the State.[41] This means that a cyberattack targeting a civilian object is sufficient for a violation of the principle.[42]

15 *Civilian object* – Considering this low threshold for a violation of the principle of distinction, it is important to know what exactly is understood as constituting 'civilian objects'. The experts in TM 2.0 confirm the expansive approach taken in IHL that a civilian object is every object not qualified as a military objective.[43] The evaluation thereof must happen in a case-by-case analysis.[44] The International Committee of the Red Cross (hereafter: "the ICRC") has defined an object as something that is "*visible and tangible*".[45] This is where things get particularly tricky regarding cyber warfare. The TM 2.0 confirms that there must be no doubt that computers, computer networks and other tangible components are objects.[46] Subsequently, if these objects are from a civilian, they are considered civilian objects which may not be targeted.[47] But what about data?

16 *Not an object* – The majority of the experts in TM 2.0 state that the IHL notion of objects does not include data, "*at least in the current state of the law*".[48] Consequently, civilian data do not

---

[38] Art. 48 AP I.
[39] Schmitt, "Rule 93", 420.
[40] Schmitt, "Rule 94 and 99", 422-423 and 434-435.
[41] Schmitt, *Tallinn Manual 2.0*, 422.
[42] Schmitt, "Rule 100", 435.
[43] Schmitt, "Rule 100", 435.
[44] *Ibidem.*
[45] ICRC, "Commentary 8 June 1977 on the Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I)," accessed March 22, 2024, https://ihl-databases.icrc.org/en/ihl-treaties/api-1977.
[46] Schmitt, *Tallinn Manual 2.0*, 437.
[47] *Ibidem.*
[48] Schmitt, *Tallinn Manual 2.0*, 437.

fall under the notion of '*civilian objects*' and targeting civilian data as such, would not constitute a violation of the principle of distinction.[49] However, targeting civilian data and as a result of that target affecting the functionality of certain civilian cyber infrastructure, could, according to the TM 2.0, nevertheless violate the principle of distinction.[50]

17 *Russia and Ukraine* – Considering again the example of the alleged cyberattack of Russia against Ukraine in 2017.[51] There were two effects established: the loss of essential data of civilian and governmental assets, and the denial of service of a nuclear power plant. Following the conclusions of the experts in TM 2.0, the loss of data would not trigger a violation of the principle of distinction in the context of an armed conflict, since it does not fall under the notion of 'object'. The target of the second effect is indeed an object, but a nuclear power plant could potentially be a lawful military objective if the other conditions for a lawful attack are fulfilled.[52] As a result, the entire operation could be accepted under IHL, even though the loss of the data and the denial of service is detrimental to Ukraine.

§3. The criticism of TM 2.0

18 *Traditional approach* – As mentioned earlier, the question regarding the principle of distinction and whether data falls under the notion of 'object' is answered negatively by TM 2.0.[53] The manual upholds a traditional approach, stating that an object must be visible and tangible.[54] A minority of the experts however, challenges this approach and is of the opinion that "*for the purposes of targeting, certain data should be considered an object"*.[55] They believe that the majority opinion excludes crucial elements from sufficient protection.[56] This exclusion results

---

[49] *Ibidem.*
[50] This approach aligns with what Harrison Dinniss calls the distinction between *"content level data"* and *"operational data"* in Harrison Dinniss, "The Nature of Objects," 39–54, https://doi.org/10.1017/S0021223714000272.
[51] See *supra* margin number 8.
[52] Schmitt, *Tallinn Manual 2.0*, 436. An object can be qualified as 'military' based on its location, nature, purpose, or use having a particular military advantage. For the other two conditions: see *infra* margin number 98.
[53] See *supra* margin number 16.
[54] Schmitt, "Rule 100", 435-437.
[55] Schmitt, *Tallinn Manual 2.0*, 437.
[56] "Focus on cyber operations that cause physical damage is not enough," Statement by the ICRC delivered by Tilman Rodenhauser, Legal Advisor, at the 7th substantive meeting of the Open-Ended Working Group on security

in an opening for deleting essential civilian datasets such as tax records, social security, and bank accounts without any legal consequences.[57] In their opinion, civilian data 'essential' to civilian society does fall under the notion of 'civilian objects' and is therefore protected under the principle of distinction.[58] It is this particular aspect of data potentially being considered an object and the consequences it would have for the principle of distinction's application, which is the main subject of the thesis.

19 *Criticism* – The approach in TM 2.0 is criticised by a minority of the TM 2.0 experts and by numerous scholars, based on a variety of reasons. Some authors suggested a potential evolutive approach of the notion 'object', while others were mostly concerned about lumping 'data' as one without distinguishing the various functions it can uphold.[59] As a result, there are several approaches on the subject matter: the approach of TM 2.0 and the various approaches of the ones providing criticism on TM 2.0.[60] Overall, the reasoning of all scholars criticising the approach in TM 2.0 is, however, threefold:

---

of and in the use of information and communications technologies 2021-2025 New York 6 March 2024, Accessed May 20, 2024, https://www.icrc.org/en/oewg-cyber-new-statement.

[57] *Ibidem.*

[58] Kubo Mačák, "Unblurring the Lines: Military Cyber Operations and International Law," accessed April 23, 2023, https://www.tandfonline.com/doi/epdf/10.1080/23738871.2021.2014919?needAccess=true&role=button.

[59] Cordula Droege, "Get off my cloud: Cyber warfare, international humanitarian law, and the protection of civilians," *International Review of the Red Cross*, no. 94 (2012): 578; Heather. A. Harrison Dinniss, "The Nature of Objects: Targeting Networks and Challenge of Defining Cyber Military Objectives," *Israel Law Review*, no. 48 (2015): 42; Humna Sohail, "Fault Lines in the Application of International Humanitarian Law to Cyberwarfare," *The Journal of Digital Forensics, Security and Law : JDFSL* 17 (2022): 1-13; Kubo Mačák, "Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law," *Israel law Review*, no. 48 (2015): 55-80; 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," *International Review of the Red Cross* 102, no. 913 (April 2020): 287-334, https://doi.org/10.1017/S1816383120000387; Michael M. N. Schmitt, "The Notion of 'Objects' During Cyber Operations: A Riposte in Defence of Interpretive and Applicative Precision," accessed May 20, 2024, https://papers.ssrn.com/abstract=2557989; Robin Geiß and Henning Lahmann, "Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space," *Israel Law Review* 45, no. 3 (November 2012): 381-99, https://doi.org/10.1017/S0021223712000179; Simon McKenzie, "Cyber Operations against Civilian Data: Revisiting War Crimes against Protected Objects and Property in the Rome Statute," *Journal of International Criminal Justice* 19, no. 5 (1 November 2021): 1165-92, https://doi.org/10.1093/jicj/mqab067; Gül, "Changing Notion of Object and Targeting Data Under the Law of Armed Conflict," 1298-1313.

[60] For the variety of approaches criticising the approach in TM 2.0: see *infra* annex 2.

1. The purpose of IHL is to protect civilians. The use of cyber warfare should not degrade that protection merely because it is not (yet) a conventional warfare method.[61]

2. If data is not considered an object, numerous operations not creating physical effects against targets would be considered lawful.[62]

3. Current State activities are already heading towards considering data an object and protecting it as such, which is evidence of the rise of a customary law rule.[63]

Regarding the latter, a customary international law (hereafter: "CIL") rule arises when there is evidence of a general practice of States, combined with a genuine belief by these States in their practice.[64]

20 *Importance of the argument* – Most of the authors involved in the debate supported the third argument, emphasising "*how States interpret rules on IHL to safeguard essential data (…) will be a litmus test for the adequacy of existing humanitarian law rules*".[65] If their statement is correct, then this practice has a large impact on the interpretation of AP I. The reason is that it is generally accepted that sources can coexist, can relate to the same topic and have an impact on one another.[66] The custom could potentially answer the previously discussed, longstanding question: can digital data be regarded as a military objective, or does it constitute an 'object' in accordance with the IHL protection of civilian objects? If an eventual new customary rule supersedes the interpretation of the article, a State could be held accountable for the violation of AP I which would be an improvement in the regulation of cyber warfare. In the previously

---

[61] ICRC, "ICRC Report 2020"; Peter Pascucci, "Distinction and Proportionality in Cyber War: Virtual Problems with a Real Solution," *Minnesota Journal of International Law*, no. 26 (2017): 419-460.
[62] Grote, "Best of Both Worlds? The Interplay between International Human Rights Law and the Law of Armed Conflict in Cyberspace"; see *infra* annex 1.
[63] Gül, "Changing Notion of Object and Targeting Data Under the Law of Armed Conflict"; Lahmann, "State Behaviour in Cyberspace"; Stephan, "Big Data and the Future Law of Armed Conflict in Cyberspace".
[64] *Jurisdictional Immunities of the State (Germany v Italy: Greece intervening),* ICJ Reports 2012 (Jurisdictional Immunities case); *North Sea Continental Shelf (Federal Republic of Germany/ Netherlands)*, ICJ Reports 1969 (North Sea Continental Shelf cases). See *infra* margin number 44.
[65] Gisel, Rodenhäuser, and Dörmann, "Twenty Years On," 287-334.
[66] Grote, "Best of Both Worlds? The Interplay between International Human Rights Law and the Law of Armed Conflict in Cyberspace".

mentioned example, it could then be established that Russia had indeed violated the principle of distinction.[67] The thesis will refer further to this argument as the 'emerging custom argument'.

21 *Lack of evidence* – The issue with the contentious argument by the authors, however, is that no scholar has presented thorough and consistent evidence for it. This is demonstrated in the scheme in annex 2: all authors mention that there is State practice, but they give barely any reference to it.[68] This makes the contentious argument questionable. To this end, the master's thesis will put theory into practice: it challenges its truthfulness, evaluating the emergence of a custom considering data an object.

2. Additional remarks and research question

22 *Notions* – Before exploring the actual research questions and the research method, it is important to define some notions which will be used in this thesis.

a. Civilian: "*In line with IHL, it understands "civilians" as all people who do not belong to the military, and "civilian objects" as (…) objects which(…) should not qualify as military objectives. While focusing primarily on the protection of civilians, sometimes (…) the protection of other persons and objects is addressed during armed conflict, such as detained or wounded soldiers or military medical facilities*."[69]

b. Custom: "*A general practice accepted as law. To establish a rule of custom, it is necessary to ascertain whether there is a general practice which is accepted as law."* [70]

---

[67] See *supra* margin number 8 and 17.
[68] See *infra* annex 2.
[69] Ar. 50 AP I; "ICRC Global Advisory Board on Digital Threats During Armed Conflicts, "Protecting civilians against digital threats during armed conflict: recommendations to States, belligerents, tech companies, and humanitarian organizations," ICRC, accessed October 25, 2023, https://www.icrc.org/en/publication/473501-protecting-civilians-against-digital-threats-during-armed-conflict.
[70] Art. 38 ICJ Statute; "ILC Report 2016," ILC, accessed October 3, 2023, https://legal.un.org/ilc/reports/2016/.

c. Cyber operation: "*The (...) operations against a computer, a computer system or network, or another connected device, through digital means. These include (...) primarily cyberattacks which are conducted as a means or method of warfare in the context of an armed conflict.*"[71]

d. Data: "*the basic element which can be processed or produced by a computer to convey information, with the exclusion of medical records, which are already protected under a specific regulation*".[72] The issue in this master's thesis involves around, more specifically, public and private civilian data.[73] This includes, but is not limited to: medical data, tax records, financial records, social security data and biometric data.[74] Medical records are, however, taken out of the scope of this research since they have a separate protection mechanism.[75]

e. IHL: "*The full range of norms regulating the conduct of armed conflict or jus in bello.*"[76] This master's thesis focusses on *jus in bello*.

f. Relevant States: Both the States who have participated in cyber operations and States who have been in a position to comment on them, the latter being relevant for the collection of evidence of *opinio juris*.

g. Source of international law: "*The historical basis of a rule, the way in which the principle became existent, the answer to the question why this is an important principle*." This is sometimes confused with the formal institution designing the law, if there exists one.[77]

---

[71] ICRC, "ICRC Global Advisory Board on Digital Threats During Armed Conflicts".
[72] Gisel, Rodenhäuser, and Dörmann, "Twenty Years On".
[73] Schmitt, "Rule 100", 437.
[74] "Scenario 12: Cyber operations against computer data," UN Cyber Toolkit, accessed December 19, 2023, https://cyberlaw.ccdcoe.org/wiki/Scenario_12:_Cyber_operations_against_computer_data#:~:text=The%20ICRC%20has%20highlighted%20medical,essential%20component%20of%20digitalized%20societies%27.
[75] Schmitt, "Rule 131 and 132", 513-515.
[76] Steven R. Ratner, "Sources of International Humanitarian Law and International Criminal Law: War/Crimes and the Limits of the Doctrine of Sources," in *The Oxford Handbook of the Sources of International Law*, ed. Jean d'Aspremont and Samantha Besson (Oxford: Oxford University Press, 2018), 915.
[77] Hugh Thirlway, *The sources of International Law: Second Edition* (Oxford: Oxford University Press, 2019), 34.

h. States' activities: All the relevant activities on the subject matter indicated in a non-exhaustive list in the Draft Conclusions on the Identification of Customary International Law (hereafter: "the DCICIL") written by the International Law Commission (hereafter: "the ILC").[78] The DCICIL provides a hierarchy between the relevant actors whose conduct is assessed when looking at State practice and *opinio juris,* - a hierarchy which is also adopted in this master's thesis.[79]

23 *Aim* – The aim of this thesis is to look for evidence of the argument made that current State activities are heading towards a CIL rule considering data an object, falling thereby under IHL's cardinal principle of distinction. The thesis does so by searching for and analysing relevant State practice and *opinio juris* on the subject matter. The research is evaluative: it evaluates whether current State activities reach the threshold for a custom – a binding legal rule – on the legal status of data.[80] It uses two internal criteria for this evaluation: *opinio juris* and State practice.[81] This research can be divided into the following research questions:

24 *Central research question* – To what extent do current relevant States' activities fulfil the conditions of a custom under IHL, which would state that data is an object under art. 52(2) of AP I? (Evaluative)

25 *Sub-question 1* – To what extent do current relevant States' activities fulfil the condition of *opinio juris* under IHL for a custom to emerge-, stating that data is an object under art. 52(2) of AP I? (Descriptive- evaluative)

26 *Sub-question 2* – To what extent do current relevant States' activities fulfil the condition of State practice under IHL for a custom to emerge-, stating that data is an object under art. 52(2) of AP I? (Descriptive-evaluative)

---

[78] ILC, *Draft Conclusions on identification of customary international law, with commentaries* (2018).
[79] See *infra* Part II.
[80] Maurice Adams and John Griffiths, "Against comparative method: explaining similarities and differences," in *Practice and theory in comparative law*, ed. Maurice Adams and Jacco Bomhoff (Cambridge: Cambridge University Press, 2012), 1-23.
[81] Lina Kestemont, *Handbook on Legal Methodology. From Objective to Method.* (Antwerp: Intersentia, 2018).

3. The relevance of the research

27 *A global issue* – The relevance of the research is threefold: first, the example of Russia and Ukraine only involved a local interruption. Similarly, a cyberattack against Georgia resulted in numerous governmental and media websites becoming inaccessible.[82] However, several experts bring up hypothetical examples of global attacks which could have worse consequences where millions of people would be without communication.[83] The potential impact of cyberattacks is thus enormous. Even if such attacks do not involve usual tools of warfare or, strictly speaking, target the whole world, the interconnectivity of our cyber networks, may result in a cyberattack against one State with consequences to be felt on a global scale.

Moreover, it is known that the world's largest militaries are increasingly investing in cyber warfare programmes.[84] The more important cyberspace becomes during warfare, the more States will attempt to degrade other States' cyber capacities, while at the same time protect their own infrastructure from potential attacks. State governments are aware that cyber operations can provide new difficulties to an armed conflict and are actively considering this development.[85] Similarly, the legal field must prepare itself for new questions which arise due to cyber warfare.

The increasing prominence and use of cyber warfare also risks reducing the protective potential of the principle of distinction: "*due to the increased societal importance of cyberspace, a person's dignity, family life and democratic freedoms are now directly targetable even without physical control over territory"*.[86] IHL cannot leave such activities in a legal vacuum, since it would decrease the level of civilian protection. Settling the case on data under IHL could prevent this. These considerations give the master's thesis important societal relevance.

---

[82] "Scenario 22: Cyber methods of warfare".
[83] See for example the scenarios in annex 1.
[84] For example: "US Army Investing Additional 25 million in Cybersecurity," US Army, accessed December 19, 2023, https://www.thedefensepost.com/2021/07/13/us-army-cybersecurity/ and Colin Clapson, "Belgium invests extra 14 billion euros in defence over the next eight years," VRT News, accessed December 19, 2023, https://www.vrt.be/vrtnws/en/2022/01/27/belgium-to-announce-major-defence-investments/.
[85] *Ibidem.*
[86] Grote, "Best of Both Worlds? The Interplay between International Human Rights Law and the Law of Armed Conflict in Cyberspace".

28 *Academic relevance* – Scholars have pointed out the need for in-depth research on State's activities.[87] They have also mentioned that official declarations of States will only gain significance in this topic, which is another reason for researching these declarations as elements of *opinio juris* and State practice.[88] The dispute around the status of data has remained unsettled, because until now, the research was theoretical, referring in an incomplete and inconsistent manner to State's activities.[89] In 2015 for example, an article attempted to fill this research gap, but its conclusion has been neglected for two reasons.[90] First, most States only started publishing reports on the topic in 2020.[91] Second, the article excluded one of the conditions for the emergence of customs: State practice.[92] The author likewise warned that the debate would likely evolve in another direction.[93] This shows that States have only been mentioned sporadically. In addition, it shows that no one has conducted research on both State opinions *and* their practice as currently settled from a legal perspective. Thorough research including new evidence of *opinio juris*, as well as of the (until now) disregarded State practice, is therefore both original and academically relevant.

29 *Upcoming initiatives* – Third and final, this thesis also has practical relevance: The UN has proclaimed that this topic remains unsettled and there is need for further research on States' opinions and activities.[94] The ICRC has recently made a similar request in their most recent report: there is need for a common understanding on how these IHL principles must be interpreted.[95] The experts of the TM 2.0 agree and made their intention clear to write a third manual, which would, among other things, look further into the legal status of data.[96] The

---

[87] Terry C. M. Hutchinson, *Researching and Writing in* Law: Third edition (Pyrmont, N.S.W.: Thomson Reuters/Lawbook Co., 2010).
[88] Lahmann, "State Behaviour in Cyberspace".
[89] For example: two other theses have also looked at this issue: the thesis of R. Verdoodt or P. Schubert. They referred however only shortly to this issue, without in-depth research, looking at only four (EU) States without an explicit method to do so and only looked at *opinio juris* without also mentioning State practice.
[90] Michael N. Schmitt and Sean Watts, "The Decline of International Humanitarian Law Opinio Juris and the Law of Cyber Warfare," *Texas International Law Journal* 50, no. 2–3 (2016): 189-232.
[91] Then, only the US had published a report.
[92] Schmitt and Watts, "The Decline of International Humanitarian Law Opinio Juris and the Law of Cyber Warfare," 189-232.
[93] Sari, "Hybrid Threats and the Law: Concepts, Trends and Implications".
[94] "Cyber Toolkit," UN, accessed March 21, 2024, https://cyberlaw.ccdcoe.org/wiki/Main_Page.
[95] ICRC, "ICRC Global Advisory Board on Digital Threats During Armed Conflicts," 3.
[96] Stephan, "Big Data and the Future Law of Armed Conflict in Cyberspace".

manual would, however, arrive only in 2030 at its earliest, leaving a timeframe for potential attacks against civilian data.[97] This research thus creates a building block for the third manual, thereby additionally reassessing the findings of the previous manuals.

The latest ICRC report emphasises the need for maximum protection of civilians and civilian data.[98] This master's thesis can be an additional help for these negotiations to draw inspiration from.[99] An additional element of practical relevance is thus that, as mentioned earlier, recognition of a custom could change the interpretation of article 52(2) AP I. It could bring a common understanding of how the principle must be interpreted in a cyber context. In summary, the issue tackled in this master's thesis has societal, academic, as well as practical relevance.

30 *Literature* – The thesis is mainly an exercise in finding evidence for an argument made by various scholars, complemented by a literature study to add the relevant background information. The literature will help the reader understand the importance of having a customary rule considering data an object. It is necessary to understand the scope of the issue described, before exploring the findings of the research. The literature study also backs up the legal nature of the thesis.

31 *Sources* – Both parts of this master's thesis rely on both primary sources (treaties, general principles, customs), as well as secondary sources (court decisions, legal doctrine). Using both sources gives an overarching analysis of the topic. For structural purposes, the explanation of how the evaluation of State's activities is done, which sources are considered and how these are presented, can be found in the second part of the thesis.[100]

---

[97] Lahmann, "State Behaviour in Cyberspace".
[98] ICRC, "ICRC Global Advisory Board on Digital Threats During Armed Conflicts," 9.
[99] Thirlway, *The sources of International Law: Second Edition*, 34.
[100] See *infra* Part II.

CHAPTER II: WHY CUSTOMARY LAW?

32 *Roadmap chapter 2* – Understanding the relevant legal rules is necessary to grasp the importance of the problem. To this end, the second chapter sets out the current sources of law applicable to cyber operations. The chapter starts with giving a short overview of the current non-binding initiatives, contrasting them with a potential binding norm, such as CIL. But why CIL? To argue in favour of CIL as the most suitable source for the contemporary challenges in cyberspace, the chapter explores the different options by comparing the sources of international law (hereafter: "IL") with CIL. This chapter provides evidence as to why a custom would be useful in the cyber context. It presents how its impact could differ from other sources, as well as from the existing non-binding initiatives. Consequently, the chapter proves why the emerging custom argument would be desirable to be found true.

1. Non-binding initiatives

§1. Two important instruments on cyber warfare

33 *Need for flexibility* – IHL is a field of IL which consists of numerous conventions.[101] Albeit robust, conventions seem to miss the ability to easily adapt to new developments in the way an armed conflict is conducted, such as the advances of technology. Accordingly, groups of experts have come together to adopt soft law, mostly in the form of behaviour manuals, as a response to these upcoming methods of war. Although it does not know a universally accepted definition, soft law in general can be defined as "*any directive or instruction, in whatever form, which creates no binding obligations for its addressees"*.[102] IL often uses soft law to address shortcomings in the current treaties and to easily adapt to upcoming challenges.[103] Similarly, it was used to address the rising challenge of cyber operations. In the following paragraphs, two of the most relevant soft-law instruments on cyber warfare are briefly mentioned.

---

[101] For example: the Geneva Conventions, the Hague Conventions, and AP I.
[102] Emily Crawford, *Non-binding Norms in International Humanitarian Law: Efficacy, Legitimacy and Legality* (Oxford: Oxford University Press, 2021), 11.
[103] Crawford, *Non-binding Norms in International Humanitarian Law*, 55 and 62.

34 *TM and TM 2*.0 – The first non-binding instruments adopted regarding attacks in cyberspace are the previously mentioned TM and TM 2.0.[104] Their publication is a response to the increasing number of attacks against States in the early 2000s.[105] As mentioned earlier, the rules included in both these manuals consisted of *lex lata*.[106] The two reports, written by experts from all over the world, provide an overview of the various cardinal IHL principles which apply to cyber operations. They add, however, both guidance and uncertainty to the debate.[107] The criticism these manuals receive suggest that they are insufficient to deal with the complexity of cyber warfare. Potentially, this could be because they are merely non-binding instruments.

35 *ICRC Report* – The second relevant non-binding instrument is the latest report of the ICRC, published in October 2023, six years after TM 2.0.[108] The ICRC is an impartial and independent organisation.[109] It states that "*in situations of armed conflict, access to digital technology can save lives"*.[110] Although this statement is indeed true, the opposite also presents a valid point: the more digitalisation, the more the potential threat increases for civilians. In its report, the ICRC emphasises that States and international organisations, NGO's, … must work together to find a common understanding regarding the interpretation of IHL and cyberattacks. This demand proves that there is still a lot of ambiguity between States' opinions on this topic and hence a lot of room for improvement and research in this area. To this end, the ICRC writes out in its report four guiding principles and multiple recommendations for the various actors part of armed (cyber) conflicts.[111] Interestingly, the report does not emphasise whether the ICRC thinks these principles should be binding. The use of the notion 'guidelines' suggests that they refer to non-binding principles.[112] The question arises whether this is sufficient to deal with the

---

[104] See *supra* margin numbers 10-11.
[105] For example: Estonia (2007), Georgia (2008), Iran (2010). Crawford, *Non-binding Norms in International Humanitarian Law*, 119.
[106] See *supra* margin number 11.
[107] See *supra* margin numbers 19-20.
[108] See *supra* margin number 29.
[109] "Who we are," ICRC, accessed May 20, 2024, https://www.icrc.org/en/who-we-are.
[110] ICRC, "ICRC Global Advisory Board on Digital Threats During Armed Conflicts".
[111] ICRC, "ICRC Global Advisory Board on Digital Threats During Armed Conflicts".
[112] Joanna Jarose, "Reconsidering the Definition of "attack" and "Damage" in Cyber Operations during Armed Conflict: Emerging Subsequent State Practice," *TheAdelaide Law Review* 1, (December 2023): 317, https://search.informit.org/doi/abs/10.3316/informit.514594046455151.

rising issue of cyber operations and what the advantages of binding principles would be.[113] The recommendations, however, ensure that there is currently no sight of treaty negotiations to regulate these operations.[114]

§2. (Dis)advantages of non-binding initiatives

36 *Advantages* – Soft law has several advantages: it is dynamic, can be adopted relatively quickly and is, as previously mentioned, easily adjustable to new situations.[115] In contrast, a treaty requires long negotiations which, at the same time, makes them sturdier. In addition, some treaties are "less binding" than others: certain provisions are formulated in quite an unclear and more suggestive than binding way, which make them difficult to enforce and make authors wonder whether they were meant to be enforced at all.[116] This, however, does not mean that the principles should not be respected.[117] An example of such a "less binding" treaty provision is the second to last sentence of article 3 of the Geneva Conventions.[118] This article encourages States in conflict to accept (part of) the Geneva Conventions as entered into force.[119] Soft law can, in its turn, be helpful in interpreting these more undefined treaty articles.

37 *Disadvantages* – Although soft law is a good addition to the already existing treaties of IHL, it raises some concerns as a standalone source of IL. First, because soft law is generally adopted by a small group of experts, potentially only a few theories per subject are heard and considered. This is especially an issue when all the experts come from a similar sociocultural background. Second, the question arises whether these instruments in practice are considered effective enough to deal with IHL challenges, since, as the title states itself: they are non-binding.[120]

---

[113] See *infra* margin number 39.
[114] ICRC, "ICRC Global Advisory Board on Digital Threats During Armed Conflicts,"; see *infra* margin number 55.
[115] Crawford, *Non-binding Norms in International Humanitarian Law*, 22-24 and 32.
[116] Crawford, *Non-binding Norms in International Humanitarian Law*, 12-13, 16 and 153.
[117] Crawford, *Non-binding Norms in International Humanitarian Law*, 13.
[118] Art. 3 Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, 12 August 1949 Geneva Convention (I).
[119] Art. 3 Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, 12 August 1949 Geneva Convention (I); Crawford, *Non-binding Norms in International Humanitarian Law*, 13.
[120] Crawford, *Non-binding Norms in International Humanitarian Law*, 1-7 and 18.

Does the severity of the conduct specifically IHL deals with not in itself imply the need for binding rules, preferably not leaving this up for debate as much as non-binding instruments do? Third, with soft law, one must always ask themselves: what were the intentions of the group introducing them? Requesting States to respect such new provisions, hoping to effectively influence States in their decision-making, or merely addressing the issue and suggesting which new measures could be adopted?[121] This question often remains unanswered, as was for example the case in the latest ICRC Report.[122] Consequently, even though the flexibility of soft law is a very attractive element for constantly developing cyber warfare, the fact that it is non-binding leaves us with new issues. Can one combine the flexibility of soft law with the appealing robustness of binding sources in IL?

38 *Effectiveness* – In comparison to the previous paragraph, a binding instrument concerning cyber warfare could entail various advantages. The binding instrument could provide certainty: the effect and the intentions of the rule would be made clear, for example in the application of the rule in case law. Second, it is not based upon negotiations by mere experts. There is thus no potential of certain theories overshadowing others. No State can, in principle, be bound against their will by a theory it does not believe in. This, in theory, helps with the fear of one sociocultural group being overrepresented during lawmaking in IHL. In addition, the ICRC, for instance, has been calling out for more development on cyber warfare for over 18 years now.[123] Considering the still uprising level of cyber operations and the unclarity around them, this shows that these non-binding instruments were generally not respected. They seem to have had little "real" effect on the behaviour of States. In comparison, violating a rule of law, as opposed to a mere non-binding principle, would have more severe consequences for a State, making a rule more effective.

39 *Summary* – In conclusion, it seems that an additional binding instrument on the issue of cyber operations will be a better fit. But why would the instrument have to be a customary rule instead of a treaty? The master's thesis has no intention on evaluating which source is "the best source

---

[121] Crawford, *Non-binding Norms in International Humanitarian Law*, 17.
[122] See *supra* margin number 35.
[123] ICRC, "ICRC Global Advisory Board on Digital Threats During Armed Conflicts," 3.

of IL". Instead, it presents the argument that, due to its flexibility and adaptability, a customary rule is the most desirable source for the challenges cyber warfare brings us. To do so, the following part compares custom to other binding sources of IL, recognised by article 38 of the Statute of the International Court of Justice (hereafter: "ICJ Statute").

2. Article 38 of the Statute of the International Court of Justice

§1. The nature of IL and the concept of sources

40 *International legislators* – One of the biggest differences between national law and IL is that at an international level there is no consistent legislator: every legal document can in theory be constructed by a different group of States, taking up the role of primary legislator.[124] Additionally, even when the Member States of, for example, the United Nations (hereafter: "the UN"), publish legislation, the international legal system does not have an unconditionally robust court system. There is no court having unconditionally binding jurisdiction regarding the interpretation or even enforcement of these regulations: the International Court of Justice (hereafter: "ICJ") remains an institution deriving from the consent of States.[125] But even though a legislator and a court system such as at the national level are absent at the international level, law nevertheless exists and is being created at the international level.[126] This is recognised in article 38 of the ICJ Statute.[127]

---

[124] Gleider Hernández, *International Law* (Oxford: Oxford University Press, 2019), 31-58; Thirlway, *The sources of International Law: Second Edition*, 2.
[125] Hernández, *International Law*, 31; Thirlway, *The sources of International Law: Second Edition*, 2. For this reason, there have often occurred theorists trying to find an alternative for international lawmaking through explicit acceptance of States. For example, a recurring question in the past therefore was often "how do we know what is and what is not law"? In the Kosovo case, judge Simma suggested making a distinction between "tolerated conduct", "permissible conduct", and "desirable conduct" instead of merely prohibition against permission. This suggestion, however, did not receive any following in practice. *Accordance with international law of the unilateral declaration of independence in respect of Kosovo (Declaration of Judge Simma)*, ICJ Reports Advisory Opinions 2010 (Kosovo Case), 480-481; *Jurisdictional Immunities of the State (Germany v Italy: Greece intervening),* ICJ Reports 2012 (Jurisdictional Immunities case); *North Sea Continental Shelf (Federal Republic of Germany/ Netherlands)*, ICJ Reports 1969 (North Sea Continental Shelf case).
[126] Article 26 VCLT; Thirlway, *The sources of International Law: Second Edition*, 10-11.
[127] Thirlway, *The sources of International Law: Second Edition*, 37.

41 *Art. 38 ICJ Statute* – Article 38 of the ICJ Statute is the written equivalent of the principle that only recognised sources can be relied upon to create IL rules.[128] The article articulates that:

1. "*The Court, whose function is to decide in accordance with international law such disputes as are submitted to it, shall apply:*
   - *International conventions, whether general or particular, establishing rules expressly recognised by the contesting States;*
   - *International custom, as evidence of a general practice accepted as law;*
   - *The general principles of law recognised by civilised nations;*

(…)
This provision shall not prejudice the power of the court to decide a case ex aequo et bono, if the parties agree thereto."[129]

42 *Importance of article 38 ICJ Statute* – Although article 38 ICJ Statute has received criticism as having a Eurocentric bias or being outdated, it is widely accepted as the traditional and authoritative statement of IL sources.[130] It is also incorporated as an Annex of the UN Charter, which is why it is highly unlikely that it will be amended in the future.[131] So, the world is bound by the same sources of IL as the world was in the 1920s, when there was no such thing as a cyberattack, let alone a cyberspace to attack.[132] Yet, this article has survived already numerous challenges in an everlasting developing international landscape.[133] This consideration makes it desirable to do any rethinking about the interpretation of cyber and IHL in concordance with article 38 ICJ.

---

[128] Thirlway, *The sources of International Law: Second Edition*, 13.
[129] Article 38 ICJ Statute; Thirlway, *The sources of International Law: Second Edition*, 11.
[130] A. Zammit Borda, "A Formal Approach to Article 38(1)(d) of the ICJ Statute from the Perspective of the International Criminal Courts and Tribunals," *European Journal of International Law* 24, no. 2 (2013): 651, https://doi.org/10.1093/ejil/cht023; Hernández, *International Law*, 32-33; Thirlway, *The sources of International Law: Second Edition*, 9-10.
[131] Art. 92 United Nations Charter, 26 June 1945; Hernández, *International Law*, 33; Thirlway, *The sources of International Law: Second Edition*, 238.
[132] Thirlway, *The sources of International Law: Second Edition*, 238.
[133] Thirlway, *The sources of International Law: Second Edition*, 239.

§2. Custom as a source in article 38 ICJ Statute

43 *Definition of custom* – CIL is considered by several authors as "*the main source of international regulation*", even though article 38 ICJ Statute does not make a hierarchy itself.[134] As derives from article 38 ICJ Statute, a CIL rule arises when a certain practice of dealing with a specific matter, becomes recognised (not necessarily unanimous) as a binding rule of law.[135] A customary rule can reflect an existing treaty provision or represent a separate obligation for all States.[136] CIL is considered desirable for solving coordination issues between different rules of law or uncertainty regarding the application or interpretation of a rule. The reason is that it looks for a degree of concurrence in practice and a corresponding belief regarding the correct way to deal with an issue.[137] In IHL there is an important role for such rules of law, not deriving directly from a treaty.[138] This is a first indication of its usefulness in the context of cyber warfare.

44 *Two elements* – For a CIL rule to arise, the ILC confirms that it must fulfil the 'two-element theory': there must be sufficient State practice, accompanied by sufficient evidence of *opinio juris*. The relationship between the two elements is best described by the ICJ in the *North Sea Continental Shelf* Cases: "*Not only must the acts concerned amount to settled practice, but they must also be such, or be carried out in such a way, as to be evidence of a belief that this practice is rendered obligatory by the existence of a rule of law requiring it. The need for such a belief, I.e., the existence of a subjective element, is implicit in the very notion of the opinio juris sive necessitatis*."[139] The elements are often intertwined; hence it is always necessary to study both:

---

[134] Fernando Lusa Bordin, Andreas Th. Müller, and Francisco Pascual-Vives, *The European Union and Customary International Law*, (Cambridge: Cambridge University Press, 2022); Carlos Iván Fuentes, *Normative Plurality in International Law: A Theory of the Determination of Applicable Rules* (Berlin: Springer, 2016), 66 and 80.
[135] North Sea Continental Shelf Cases; ILC, *Draft Conclusions on identification of customary international law, with commentaries* (2018), conclusion 2 and 9; La Haye, *War crimes in internal armed conflicts*, 49 and 55; Thirlway, *The sources of International law: Second Edition*, 11.
[136] Marija Dordeska, "The process of International Law-making: The relationship between the International Court of Justice and the International Law Commission," *ICLR* 15, no. 1 (2015): 14; La Haye, *War crimes in internal armed conflicts*, 49.
[137] Joseph A. Maxwell, *Qualitative Research Design. An Interactive Approach* (New York: Sage, 2013); Thirlway, *The sources of International Law: Second Edition*, 64.
[138] For example: International Military Tribunal for the Trial of German Major War Criminals recognizing the Hague Conventions as declaratory of the customs of war. *Case concerning military and paramilitary activities in and against Nicaragua (Nicaragua v. United States)*, ICJ Reports 1986 (Nicaragua case); Prosecutor v. Tadić, ICTY 1999 (Tadić case); Thirlway, *The sources of International Law: Second Edition*, 208.
[139] North Sea Continental Shelf Cases, §77.

one cannot have a conclusion with one of the elements missing.[140] Both constituent elements are considered equally important for the emergence of a custom.[141]

45 *Same coin* – The two-element theory does not actually require two elements. It is more about two sides of the same coin: jurists look for practice and accompanying this practice, *opinio juris* must exist.[142] The State practice must clearly represent their belief in their own behaviour. States cannot be doing it out of mere tradition, for example.[143] Even though before this was often questioned, the ILC has now confirmed that State practice and *opinio juris* can be found in the same sources.[144] As a result, the boundaries between the evidence of these two are rarely explicitly delineated, they are merely looked at in a different manner.[145] In the same manner, courts, for instance, do not separately address the evidence they analysed when finding custom. They do not say "X helped to support reasoning 1".[146] Because of this lack of precise explanation, some authors criticise the CIL method of lawmaking.[147]

46 *State practice* – State practice is defined as "*examples of consistent conduct in harmony with the alleged custom*".[148] It can primarily be found in the actions of a State at a national level.[149] Additional conditions are that the practice must be extensive, virtually uniform, and it must

---

[140] Thirlway, *The sources of International Law: Second Edition*, 71.
[141] Raphaël van Steenberghe, "Sources of International Humanitarian Law and International Criminal Law: Specific Features," in *The Oxford Handbook of the Sources of International Law*, ed. Jean d'Aspremont and Samanta Besson (Oxford: Oxford University Press, 2018), 897; see *infra* margin number 80-81.
[142] See *infra* margin number 71.
[143] Giovanni Distefano, *Fundamentals of Public International Law: A Sketch of the International Legal Order*, (Brill: Nijhoff, 2019), 321-322, https://doi.org/10.1163/9789004396692; Roozbeh (Rudy) B. Baker, "Customary international law in the 21st Century: Old Challenges and New Debates," *European Journal of International Law* 21, no. 1 (1 February 2010): 173–204, https://doi.org/10.1093/ejil/chq015.
[144] Michael Byers, *Custom, Power and the Power of Rules: International Relations and Customary International Law* (Cambridge: Cambridge University Press, 1999), 136.
[145] László Blutman, "Conceptual Confusion and Methodological Deficiencies: Some Ways That Theories on Customary International Law Fail," *European Journal of International Law* 25, no. 2 (1 May 2014): 529, https://doi.org/10.1093/ejil/chu034.
[146] Stephen J. Choi and Mitu Gulati, "Customary international law: how do courts do it?," in *Custom's Future: International Law in a Changing World*, ed. Curtis A. Bradley (Cambridge: Cambridge University Press, 2016), 125; Ryan M. Scoville, "Finding Customary International Law," *Iowa Law Review* 101, (2016): 1896-1897.
[147] See *infra* margin number 60.
[148] Scoville, "Finding Customary International Law," 1897.
[149] David Haljan, *Separating powers: international law before national courts* (Den Haag: Asser Press, 2013), 214-215; Thirlway, *The sources of International Law: Second Edition*, 66.

include practice of which the State itself is aware.[150] Consequently, it is important to consider the context in which the practice takes place.[151] The DCICIL believe that the relevant practice can appear both as verbal and physical acts, as long as it appears by a State acting in the exercise of one of its functions.[152] Overall, there is a broad conception of the notion "State practice".[153] Conclusion 6, §2 of the DCICIL provides a non-exhaustive list of examples of State practice.[154]

47 *Opinio Juris – Opinio juris* is defined as "*the view that what is involved is required by the law, or by necessity*."[155] It requires that "*the practice in question must be undertaken with a sense of legal right or obligation*".[156] In essence, evidence is necessary of a certain practice considered justifiable under international law by a State.[157] There must be a shared belief that a certain norm is the legally valid norm in a certain context.[158] This idea that a specific belief must be supported by State practice entails that States maintain and apply their power in the creation of international obligations: no overarching system can produce obligations for them without them consenting to it in a certain way.[159] Finally, *opinio juris* can occur in various forms, which the ILC has presented a non-exhaustive list in its conclusions in 2018.[160]

---

[150] Byers, *Custom, power and, the power of rules*, 156; La Haye, *War crimes in internal armed conflicts*, 49.
[151] Byers, *Custom, power and, the power of rules*, 156.
[152] ILC, *Draft Conclusions*, conclusions 5 and 6, §1; Haljan, *Separating powers*, 215; Omri Sender and Michael Wood, "A Mystery No Longer? Opinio Juris and Other Theoretical Controversies Associated with Customary International Law," *Israel Law Review* 50, no. 3 (November 2017): 303-304, https://doi.org/10.1017/S0021223717000115.
[153] Nicaragua case; Monica Hakimi, "Custom's method and process in custom's future," in *Custom's Future: International Law in a Changing World*, ed. Curtis A. Bradley (Cambridge: Cambridge University Press, 2016), 168.
[154] Byers, *Custom, power and, the power of rules*, 134-135.
[155] ILC, *Draft Conclusions*, conclusions 5 and 6, §3; Haljan, *Separating Powers*, 214.
[156] Choi and Gulati, "Customary international law: how do courts do it?," 118-119; Brian D. Lepard, *Customary International Law: A New Theory with Practical Applications*, (Cambridge: Cambridge University Press, 2010), 34.
[157] ILC, *Draft Conclusions*, conclusion 6, §2. Further explanation of which elements in particular are of importance for State practice can be found in part II.
[158] ILC, *Draft Conclusions*, conclusion 9, §1.
[159] North Sea Continental Shelf Cases; Baker, "Customary international law in the 21st Century," 179; Blutman, "Conceptual Confusion and methodological deficiencies", 539; Thirlway, *The sources of International Law: Second Edition*, 84.
[160] La Haye, *War crimes in internal armed conflicts*, 49; Thirlway, *The sources of International Law: Second Edition*, 90.

48 *Timeframe* – There is no need for a certain period to pass before one can speak of a custom. If the issue concerned appears often, in different contexts, and the consequences given to it appear to be quite similar, the timeframe in which it occurs can be limited.[161] The ICJ confirmed this, stating that: "*the passage of only a short period of time is not necessarily, or of itself, a bar to the formation of a new rule of customary law...*".[162] In specific circumstances, containing fundamental change, a CIL rule can thereby develop relatively quick.[163] Potentially, this is the case for the emerging custom argument.

49 *State 'action'* – It is not required for a State to have engaged in particular conduct before its opinion becomes relevant for *opinio juris*.[164] For example with nuclear weaponry, not all States were engaged in relevant conduct. However, this does not mean that States could not be victimised by the actions of other States. As a result, potential victims have a relevant belief on the topic to take into consideration.[165] Considering that not every State conducts cyber operations, yet every State is a potential victim through the interconnectivity of cyberspace, makes it desirable to consider them relevant in CIL for identifying a new rule.

50 *Specially affected* – For a general custom to emerge, it is not required to have relevant practices from all over the world of every State: widespread and consistent practice suffices.[166] Important here is the notion of 'specially affected States'. In previous decades, this notion was used to define the most "civilised" States. However, this term changed *de facto* more towards "most powerful" States, opposing a diverse approach and particularly opposing the global South.[167] This consideration has made the notion controversial over the years.[168] Considering the

---

[161] Byers, *Custom, power and, the power of rules*, 7, 18 and 130.
[162] Byers, *Custom, power and, the power of rules*, 142.
[163] Thirlway, *The sources of International Law: Second Edition*, 69.
[164] ILC, *Draft Conclusions*, conclusion 10; Lepard, *Customary International Law: A New Theory with Practical Applications*, 9. Further explanation of which elements in particular are of importance for *opinio juris* can be found in part II.
[165] Sender and Wood, "A mystery no longer?," 305; Brian Lepard, "Reexamining Customary International Law" in *Custom's Future: International Law in a Changing World*, ed. Curtis A. Bradley (Cambridge: Cambridge University Press, 2016), 86.
[166] North Sea Continental Shelf Cases, §73.
[167] ICRC, "Study on Customary International Humanitarian Law: A Contribution to the Understanding and Respect for the Rule of Law in Armed Conflict," *International Review of the Red Cross,* no. 87 (2005): 175-212.
[168] ILC, *Draft Conclusions*, conclusion 8, §2; Thirlway, *The sources of International Law: Second Edition*, 74.

interconnectedness of cyberspace, this notion of "specially affected States" is arguably useless in the current topic: every State can potentially be affected, even though not all of them conduct their own cyber operations. Accordingly, this master's thesis did not make use of the doctrine of "specially affected States" to identify the relevant States to analyse. Instead, it used three other objective conditions.[169]

The previous paragraphs have shown that some elements of CIL make it a relevant source in IHL, and consequently in cyber warfare. But what about the two other primary sources in article 38 ICJ Statute?

§3. Custom *versus* treaties

51 *Core principles* – Another binding source mentioned in article 38 ICJ Statute, are conventions.[170] Their binding force relies upon the *pacta sunt servanda*- principle.[171] This principle states that: "*every treaty is binding upon the parties to it and must be performed by them in good faith*".[172] Each party is rest assured that the other parties, because of the binding nature of the treaty, will execute the provisions of the treaty even if it is inconvenient to them.[173] In addition, there is the principle of relative effect: only those States that accept the treaty, will be bound by it. For them, the rules will be considered law.[174] On the other hand, when signing or ratifying a treaty, States can enter reservations to it: they can decide not to accept one or more treaty obligations. Consequently, a single treaty can apply to different States in various versions.[175]

---

[169] Thirlway, *The sources of International Law: Second Edition*, 74.
[170] The notions "convention" and "treaty" are used interchangeably in this master's thesis. Nancy Kontou, *The Termination and Revision of Treaties in the Light of New Customary International Law, Oxford Monographs in International Law* (Oxford: Clarendon, 1994), 20-21; Rebecca Crootof, "Change without Consent: How Customary International Law Modifies Treaties," *Yale Journal of International Law* 41, no. 2 (2016): 239.
[171] Art. 26 VCLT; Crootof, "Change without Consent," 239; Thirlway, *The sources of International Law: Second Edition*, 10-11.
[172] Art. 26 VCLT.
[173] Mark Eugen Villiger, *Customary International Law and Treaties: A Manual on the Theory and Practice of the Interrelation of Sources* (Leiden: Martinus Nijhoff Publishers, 1997), 129-130; Thirlway, *The sources of International Law: Second Edition*, 37.
[174] Crootof, "Change without Consent," 247.
[175] Thirlway, *The sources of International Law: Second Edition*, 45-46 and 50.

52 *Comparison with custom* – The previous paragraph provides an opportunity to illustrate some advantages of CIL over treaties in cyberspace. First, a CIL rule, as opposed to treaties, exists in only one form: either you are bound by it, or you are a persistent objector. In addition, adjusting treaties to recent developments is difficult as a result of the principle of *pacta sunt servanda*. A treaty can only be changed by another treaty.[176] Moreover, finding consensus on a new topic has, as appeared in the past, been very difficult and can take quite a long time, since successive ratifications in numerous States are often required. CIL rules on the other hand, develop at an unprecedented rate because of the more interconnectedness and contacts between States.[177] Similarly, cyber operations are developing at an unprecedented rate and it seems that waiting for an agreement on a treaty could have detrimental consequences.

53 *Agreement* – One of the counterarguments used against CIL is the fact that "*International law governs relations between independent States. The rules of law binding upon States therefore emanate from their own free will as expressed in conventions (…)*."[178] It is, however, untrue that custom does not derive from agreement.[179] It is made up of two elements: State practice and *opinio juris*. This final element requires that for there to be a custom, there must be a perception that something is required by law or necessity.[180] *Opinio juris* shows that there is an element of agreement in CIL, but with the lack of the formalities in treaty-making, CIL is arguably easier to evolve to respond to challenging situations like cyber warfare.[181] This paragraph presents a third argument in favour of CIL for the current topic.

54 *Generally binding* – A fourth advantage of custom over treaties consists in the fact that custom is generally binding on all States, whether they are 'responsible' for the development of the

---

[176] Crootof, "Change without Consent," 238-239 and 243.
[177] Crootof, "Change without Consent," 246-247; Avidan Kent and Jamie Trinidad, "International Law Scholars as *Amici Curiae* : An Emerging Dialogue (of the Deaf)?," *Leiden Journal of International Law* 29, no. 4 (December 2016): 1086, https://doi.org/10.1017/S0922156516000510.
[178] *SS Lotus (France v. Turkey),* PCIJ, judgement, 1927, 18 (SS Lotus case).
[179] Villiger, *Customary International Law and Treaties*, 62.
[180] See *supra* margin number 47.
[181] Thirlway, *The sources of International Law: Second Edition*, 13; Jonathan L. Black-Branch, *The treaty prohibitions on Nuclear Weapons: legal challenges for military doctrines and deterrence policies*, (Cambridge: Cambridge University Press, 2021), 118.

custom or not.[182] This way, a customary rule can be essential to reach non-State parties to a treaty having gained the status of customary law.[183] It also lowers the burden of proof for a State during a dispute: instead of having to provide evidence of a certain treaty rule existing and the opposing State to be bound by it, the accusing State merely must establish that the customary rule exists.[184]

There are two exceptions to this:

1. Persistent objectors: a State can, explicitly disapproving of a rule while it is still in the process of becoming such a rule, become a persistent objector. Consequently, the State can then opt out of the application of the rule, even after it has acquired the status of a rule of general custom.[185] This exception has rarely been used in practice, however.

2. Local, special, or regional customs: these customs are merely applicable to a specific group of States, bound for geographical or other specific reasons.[186] An example hereof is the practice of diplomatic asylum in South America: it is a purely local rule which is not used in favour or against a State outside this area.[187]

55 *Jus cogens* – A fifth advantage to mention regards the concept of *jus cogens*. *Jus cogens* shows that some CIL rules cannot be deviated from by a treaty.[188] In addition, when a treaty explicitly excludes the application of a certain rule of CIL, the rule continues to exist in international law and binds other States.[189] Certainly in an IHL context and with the amount of cyber operations still growing concerningly, this is an attractive element to consider. Of course, custom and treaties can also coexist without conflict: if several norms involve the same issue, they must be

---

[182] Thirlway, *The sources of International Law: Second Edition*, 61.
[183] La Haye, *War crimes in internal armed conflicts*, 49.
[184] Thirlway, *The sources of International Law: Second Edition*, 63.
[185] Thirlway, *The sources of International Law: Second Edition*, 100.
[186] ILC, *Draft Conclusions*, conclusion 16.
[187] Thirlway, *The sources of International Law: Second Edition*, 103.
[188] Art. 53 VCLT; Kontou, *The Termination and Revision of Treaties in the Light of New Customary International Law*, 31; Thirlway, *The sources of International Law: Second Edition*, 153.
[189] Kontou, *The Termination and Revision of Treaties in the Light of New Customary International Law*, 22; Villiger, *Customary International Law and Treaties*, 59, 128, 136 and 231.

interpreted to assist one another.[190] Over time, when a cyber treaty could arise, it could lean on a previously defined CIL rule.

The previous paragraphs present reasons to prefer a CIL rule over a treaty regarding the legal gap in relation to cyberwarfare. The ICRC also has explicitly stated that a treaty on cyber warfare is currently not possible.[191] But what about general principles?

§4. Custom *versus* general principles of international law

56 *Similarities* – General principles are defined as principles which are universally and officially approved by "*States' belonging to the "main" legal doctrines, the so-called 'civilised nations'*".[192] What the definition precisely means, is up for debate.[193] Unlike for the adoption of international conventions, there is no format for the emergence of general principles.[194] This makes it hard to distinguish them from CIL, since CIL and general principles have similar features. A first similarity with customary law, recognisable in this definition, is that they both are a bit "obscure". They are both unwritten and no relevant exhaustive list exists at the international level.[195] There is no consensus as to which legal principles are truly considered

[190] Nicaragua Case as cited in Black-Branch, *The treaty prohibitions on Nuclear Weapons*, 119 and 128; Thirlway, *The sources of International Law: Second Edition*, 152; Villiger, *Customary International Law and Treaties*, 157, 230 and 286; Sotirios-Ioannis Lekkas and Panos Merkouris, "Interpretation of International Law: Rules, Content, and Evolution," *Netherlands International Law Review* 69, no. 2 (September 2022): 184, https://doi.org/10.1007/s40802-022-00226-w.
[191] See *infra* margin number 60.
[192] Hye-Ryon Son et al., "Reassessment of the "General Principles of Law" Referred to in Article 38(1)(c) of the ICJ Statute," *International Studies (New Delhi)* 59, no. 2 (2022): 152, https://doi.org/10.1177/00208817221100912.
[193] Craig Eggett, "The Role of Principles and General Principles in the "Constitutional Processes" of International Law," *Netherlands International Law Review* 66, no. 2 (July 2019): 198, https://doi.org/10.1007/s40802-019-00139-1.
[194] Paolo Palchetti, "The Role of General Principles in Promoting the Development of Customary International Rules," in *General Principles and the Coherence of International Law,* ed. Paolo Palchetti (Leiden: Brill Nijhoff, 2019), 47-59, https://doi.org/10.1163/9789004390935_005.
[195] Thomas Kleinlein, "Customary International Law and General Principles: Rethinking Their Relationship," SSRN Scholarly Paper, accessed March 22, 2024, https://doi.org/10.2139/ssrn.2923964.

part of IL.[196] Furthermore, for general principles and CIL, there is a requirement as to the existence of a "type of" practice.[197]

57 *Custom vs. general principles* – Differentiating general principles from CIL is not easy.[198] For example, the ICJ itself does not always distinguish between general principles and CIL in its case law. The court often uses the term "general IL", which includes both.[199] Not only the ICJ, but also several authors confirm having difficulties with distinguishing the two.[200] Nevertheless, most of the legal doctrine does believe that they are two distinct sources. Accordingly, custom is based on State practice that must be general and uniform.[201] This is not required for general principles, irrespective of whether they originated in national law or IL.[202] General principles need some form of acceptance by the international community: they must be "*recognised by civilised nations*", but that recognition must not necessarily lie in a specific existence of a general practice.[203] General principles can initiate the process of creating a new customary law rule.[204] They can be a starting point for CIL, but custom needs more strict evidence. Perhaps, this makes custom more trustworthy, which is why it is relied upon much more than general principles at the international law level. Given the potential consequences that the emerging custom argument can have, the requirement of sufficient evidence in CIL makes it favourable.

---

[196] Son et al., "Reassessment of the "General Principles of Law" Referred to in Article 38(1)(c) of the ICJ Statute," 155.
[197] Article 38, 1, b and c ICJ Statute; Kleinlein, "Customary International Law and General Principles," 10 and 16.
[198] Imogen Saunders, *General Principles as a Source of International Law: Art. 38(1)(C) of the Statute of the International Court of Justice* (London: Bloomsbury Publishing, 2021), 53.
[199] Johannes Antonius Maria Klabbers, and August Reinisch, "Sources of international organizations law: reflections on accountability" in *The Oxford Handbook on the Sources of International Law*, ed. Jean d'Aspremont and Samantha Besson (Oxford: Oxford University Press, 2017), 987-1006.
[200] Kleinlein, "Customary International Law and General Principles," 17.
[201] See *supra* margin numbers 43-44.
[202] Palchetti, "The Role of General Principles in Promoting the Development of Customary International Rules," 47.
[203] Odile Ammann, *Domestic Courts and the Interpretation of International Law: Methods and Reasoning Based on the Swiss Example* (Leiden: Brill Nijhoff, 2020), 148, https://doi.org/10.1163/9789004409873; Palchetti, "The Role of General Principles in Promoting the Development of Customary International Rules," 47.
[204] See *supra* margin numbers 55-56.

3. Interim conclusion: the relevance of the emerging custom argument: why is it desirable to be found true?

58 *The issue* – The first part of the thesis has set out the current inconsistency on whether data is an object. TM 2.0, the most authoritative (non-binding) document on the topic, states that this is not the case "*at least in the current state of law*".[205] It finds that data can be protected only when the attack disrupted the cyber infrastructure itself.[206] Several authors do not agree. In general, they put out three arguments for their disagreement. By far the most interesting one, is them upholding that "*State practice is already heading towards considering data an object under CIL*".[207] The authors do not, however, present conclusive evidence for their statement.

59 *The relevance* – To explain why it is important whether this argument is indeed found true, the chapter has explained the relevance of CIL in general. It has compared the general theory to two other sources mentioned in article 38 ICJ Statute: conventions and general principles. In comparison to a potential cyber treaty, it found that CIL has the potential of binding all States, not just the one agreeing to the treaty. This makes it desirable in an IHL and especially, cyberspace context: interconnectivity requires all States to be on the same page.

In comparison to general principles, CIL requires more robust evidence, which is certainly desirable in an IHL context, considering the severity of the potential consequences in this legal field. The fact that authors refer to CIL in this topic, is an argument itself for why it is relevant in cyber warfare.

Overall, the following figure presents the features of cyber warfare and how the three primary sources of IL correspond to them. As a result, this thesis argues that CIL is indeed the most desirable source to have in a cyber warfare context. The result of the comparison significantly increases the importance of the emerging custom argument.

---

[205] Schmitt, *Tallinn Manual 2.0*, 437.
[206] *Ibidem.*
[207] See *supra* margin numbers 19-20.

	Rapidly evolving	Interconnectivity: considering potential victims	Need for certainty: clear evidence of agreement
Conventions	Not easily adjustable due to formalities	Not everyone considered: only those participating	Yes: by virtue of formalities
General principles	Easily evolving	In principle, everyone considered	No: "some form of acceptance", but rather unclear criterium
CIL	Easily evolving	In principle, everyone considered	Yes: *opinio juris* and State practice required

Figure 1: comparison of cyber warfare-features and IL primary sources

60 *Criticism on CIL* – CIL, however, is not faultless. On the contrary, because of its informal and continuous process of lawmaking, it is one of the most discussed topics in IL.[208] Criticism on the lack of a clear operating method has occurred in various forms, through various authors and over various periods of time. One could say they have become custom themselves. The ILC, under leadership of Special Rapporteur sir Michael Wood, has presented commentaries and conclusions to tackle these questions in 2018.[209]

For example, because of its informal law-creating method, its lack of formalities, and the nonexistence of an overarching foreign system, the question arises whether CIL will remain relevant.[210] After all, authors claim that there is a trend towards increasing the importance of written sources, since this comes closer to the belief of having a legitimate and authoritative source of law.[211] They argue that all currently applicable customary rules are also codified in

[208] Andreas Th. Müller, "The direct effect of Customary Internation Law: The Treaty Analogy' and Its Limits," in *The EU and customary international law*, ed. Bordin et al. (Cambridge: Cambridge University Press, 2022); Fuentes, *Normative Plurality in International Law*, 66; Jean d' Aspremont, "Non-State Actors and the formation of international customary law: unlearning some common tropes," in *Non-State Actors and the formation of customary international law*, ed. Ian Scobbie and Sufyan Droubi (Manchester: Manchester University Press, 2020), 129; Monica Hakimi, "Making sense of customary international law," *Michigan Law Review* 118 (2020): 1487-1488; Scoville, "Finding Customary International Law," 1897.
[209] Hakimi, "Making sense of customary international law," 1497.
[210] Byers, *Custom, power and, the power of rules*, 35.
[211] Haljan, *Separating powers*, 211-212.

treaties. Thereby the custom does not disappear but coexists with the treaty provision.[212] The question is then what the additional impact of custom is. Perhaps the only reason the treaty provision came to life, is because the custom existed beforehand.[213] Applying this reasoning to the topic of cyber operations, the ICRC has opined that a cyber treaty is currently nowhere near possible. Perhaps over time, if there is indeed a custom considering data an object, this could change through this custom itself.

61 *A clear form and a mixed method* – Although the process of customary lawmaking is not spared from criticism, CIL has played a vital role in IL and will play an equally important role in the future.[214] While the informal process of customary law seemed to be the desirable aspect at first, it is perhaps not the true reason why customary law gains such important status. The lack of clear theory has been criticised for centuries, with numerous theories built around it to simplify it.[215] These theories on the other hand, have likewise not always used a concise method, with the ICJ serving as a prime example.[216] The best conclusion therefore seems that the specific form of CIL is clearly laid down (*opinio juris* and State practice), but the method on how to identify these elements can differ regarding the case.[217] In addition, the biggest issue with these criticisms seems their entire focus on how to analyse what States do, instead of looking at what they should do.[218] That way, CIL's true power may lie in it being an instrument for States to achieve morally praiseworthy goals, if they want to, without too strict formalities.[219] This is a

---

[212] Byers, *Custom, power and, the power of rules*, 4; Joel P. Trachtman, "The growing obsolescence of customary international law," in *Custom's Future: International Law in a changing world*, ed. Curtis A. Bradley (Cambridge: Cambridge University Press, 2016), 174 and 194.
[213] Crootof, "Change without Consent," 241 and 245-247.
[214] Hanna Bourgeois and Jan Wouters, "Methods of identification of international custom: a new role for opinio juris?" in *Global Justice, Human Rights and the Modernization of International Law*, ed. Riccardo Piscillo Mazzeschi and Pasquale de Sena (Cham: Springer international Publishing, 2018), 346; Lepard, *Customary International Law: A New Theory with Practical Applications*, 379; *contra* Trachtman, "The growing obsolescence of customary international law," 174.
[215] Green, *The persistent objector rule in international law*, 252; Hakimi, "Making sense of customary international law," 1489.
[216] Hakimi, "Custom's Method and Process: Lessons from Humanitarian Law," 170.
[217] Giovanni Distefano, *Fundamentals of Public International Law: A Sketch of the International Legal Order*, (Brill: Nijhoff, 2019), 338.
[218] Green, *The persistent objector rule in international law*, 252; Hakimi, "Making sense of customary international law," 1491-1492 and 1504.
[219] Lepard, *Customary International Law: A New Theory with Practical Applications*, 379; Sender and Wood, "A mystery no longer?," 305.

final argument for why CIL could be relevant in the context of cyber warfare. States could achieve considering data an object without having to sit around the table all together.

It is also not the case that this focus on what States believe should be the law, would result in them making highly controversial claims for the sake of it: they know what legal consequences can come out of this.[220] CIL will still only arise when other States are willing to make the same statement: they must reason with one another.[221] Returning now, to the actual research on State's activities: are they reasoning with one another on cyber warfare? Are they truly considering data as an object?

[220] Hakimi, "Custom's Method and Process: Lessons from Humanitarian Law," 171.
[221] *Ibidem.*

PART II: STATES' ACTIVITIES PUT TO THE TEST

CHAPTER I: GENERAL INFORMATION ABOUT THE TEST

62 *Form before method* – As mentioned earlier, there is considerable criticism on the lack of a general procedure to look at evidence for CIL.[222] This master's thesis argues that the debate unfairly casts a spotlight on the lack of clear methodology. The thesis states that CIL must consist of a clear form - a combination of *opinio juris* and State practice - but that the method on how this evidence is found can differ depending on the case.[223] Consequently, the following paragraphs will explain the method that is suitable for this research and on what theory this method is based.[224]

63 *Induction* – Stefan TALMON has written a very clear article on the methods used by the ICJ to decide on the existence of a CIL rule.[225] In this article, he states that the primary method the ICJ used, is the inductive method: *"inference of a general rule from a pattern of empirically observable individual instances of State practice and* opinio juris*. Induction is a process of going from the specific to the general. It is a systematic process of observation and empirical generalization*."[226] In short it looks for generalities inside specificities, evidence of a common denominator among specific cases.[227] This method is desirable, because it enables us to reflect on multiple States at once inside a limited timeframe.[228] TALMON confirms, however, that this method, cannot always be used. When a topic came too recently to exist, it is difficult to find

---

[222] See *supra* margin number 60.
[223] See *supra* margin number 61.
[224] For structural purposes, some more in-depth comments on the methodology are presented in annex 3.
[225] Stefan Talmon, "Determining Customary International Law: The ICJ's Methodology between Induction, Deduction and Assertion," *European Journal of International Law* 26, no. 2 (May 2015): 417–43, https://doi.org/10.1093/ejil/chv020.
[226] *Ibidem.*
[227] ILC, *Draft Conclusions*; *Contra* Monica Hakimi, "Making Sense of Customary International Law," *Michigan Law Review* 118, no. 8 (June 2020): 1487-1538.
[228] Christian Marxsen, "What Do Different Theories of Customary International Law Have to Say About the Individual Right to Reparation Under International Humanitarian Law?" Accessed May 17, 2024. https://www.zaoerv.de.

generalities amongst the specificities.[229] In that case, he suggests that the ICJ uses deduction: specifying the application of a general rule to a particular case.[230]

64 *Contrasting opinions* – While TALMON's theory described as above receives recognition, not everyone agrees with it. For example, the ILC's Special Rapporteur Michael WOOD and Omri SENDER have disapproved of his position that the ICJ sometimes uses a deductive method instead of induction.[231] They hold onto the ILC's draft conclusions themselves, stating that the only method used by the ICJ is the inductive method.[232] In a response to their disagreement however, TALMON refers to a report written by the ILC Chairman, Bernd H. NIEHAUS, in which he states that the ILC is aware of the criticism voiced regarding the *Arrest Warrant* Case, because of the case being assessed on deductive reasoning.[233] Talmon hereby concludes that the practice of finding and determining CIL rules is more complex than what the ILC Draft Conclusions explain it to be.[234] Importantly, their disagreement primarily involves the method used to recognise CIL, not about the type of sources used within that method.[235]

65 *Hakimi's theory* – Agreeing with TALMON, Monica HAKIMI takes the view that the ILC's Draft Conclusions do not reflect reality.[236] However, that is the only element the two authors

---

[229] Talmon, "Determining Customary International Law: The ICJ's Methodology between Induction, Deduction and Assertion,"; *contra* Omri Sender and Michael Wood, "ICJ and Customary International Law: a reply to Stefan Talmon," accessed March 22, 2024, https://www.ejiltalk.org/the-international-court-of-justice-and-customary-international-law-a-reply-to-stefan-talmon/.
[230] Talmon ends his article by arguing that he believes the ICJ actually in most cases uses neither of these methods, but uses assertion instead. This has not been confirmed by the ICJ, nor by the ILC, so this current theory is not followed in the thesis.
[231] Michael Wood and Omri Sender, "The International Court of Justice and Customary International Law: A Reply to Stefan Talmon," EJIL Talk, accessed May 17, 2024, https://www.ejiltalk.org/the-international-court-of-justice-and-customary-international-law-a-reply-to-stefan-talmon/.
[232] ILC, *Draft Conclusions*, conclusion 2; Michael Wood and Omri Sender, "The International Court of Justice and Customary International Law: A Reply to Stefan Talmon," EJIL Talk, accessed May 17, 2024, https://www.ejiltalk.org/the-international-court-of-justice-and-customary-international-law-a-reply-to-stefan-talmon/.
[233] UN General Assembly, Sixth Committee, *UN Doc. A/C.6/68/SR.17*, (8 November 2013), 6, §20; Stefan Talmon, "Determining Customary International Law: the ICJ's Methodology and the Idyllic World of the ILC," EJIL Talk, accessed May 17, 2024, https://www.ejiltalk.org/determining-customary-international-law-the-icjs-methodology-and-the-idyllic-world-of-the-ilc/.
[234] Stefan Talmon, "Determining Customary International Law: the ICJ's Methodology and the Idyllic World of the ILC," EJIL Talk, accessed May 17, 2024, https://www.ejiltalk.org/determining-customary-international-law-the-icjs-methodology-and-the-idyllic-world-of-the-ilc/.
[235] See *supra* margin number 62.
[236] Hakimi, "Making Sense of Customary International Law," 1489.

agree upon. HAKIMI defines the ILC's approach as "the rulebook conception": contemporary beliefs on CIL presuppose that CIL can only consist of generally applicable rules based on the two-element test.[237] She continues by stating that even authors who criticise the approach of the ILC, like TALMON does, nevertheless still adhere to the 'rulebook conception' to a certain level.[238] Instead of adding to the criticism on the inductive method presented by the ILC like TALMON, she presents a whole new approach: one based on a "true" reflection of what CIL is in real life.[239] By doing so, she concludes that CIL is not based on the two-element test as generally applicable criteria but that it is more organically based on variable criteria and that they can result in more than mere rules.[240] The author of this master's thesis believes that HAKIMI's theory presents the best understanding of the informal character of CIL and how it comes to exist. However, the author also believes that HAKIMI mistreats the two-element test as a type of 'rule of recognition'. HAKIMI presents this test as an element in a method to find CIL and therefore she disregards it. The author of this master's thesis believes on the other hand that the two-element test is not about a certain method, it is about the form in which CIL arises: CIL indeed emerges in a very informal manner, but the author disagrees with HAKIMI that the two-element test is an issue for CIL to emerge informally. As a result, even though her theory is an interesting one, this thesis chooses to remain with the theory of Talmon.

66 *Four situations* – TALMON identifies four situations where induction seems impossible.[241] These four situations are the following: when State practice is nonexistent, when State practice is too disparate, when the *opinio juris* cannot be established, and when there is a discrepancy between State practice and *opinio juris*. Applying his reasoning to the current analysis, the author draws the following conclusions:

---

[237] Hakimi, "Making Sense of Customary International Law," 1490.
[238] Hakimi, "Making Sense of Customary International Law," 1497-1500.
[239] Hakimi, "Making Sense of Customary International Law," 1491.
[240] Hakimi, "Making Sense of Customary International Law," 1506, 1510, 1516, and 1529.
[241] Talmon, "Determining Customary International Law: The ICJ's Methodology between Induction, Deduction and Assertion," 421-422.

1. State practice is non-existent: the authors of the emerging custom argument claim that there is State practice. Their argument is the starting point of this research, so the author must assume that there is practice.

2. State practice is conflicting or too disparate and thus inconclusive: this can only be found after the start of the analysis.

3. The *opinio juris* cannot be established: Talmon explains that this is mostly an issue when States refuse to interfere in the discussion. Talmon defines this as 'negative practice' or 'omission'. By doing so, the States vacillate whether they agree. That is not the case here, because one of the factors on which the States were chosen, was ensuring that they have made a statement.

4. There is a discrepancy between State practice and *opinio juris*: again, this can only be found after the start of the analysis.[242]

As a result, the research will start by looking at State practice, followed by investigating whether evidence can be found of a belief that these actions are legally required.[243]

67 *Choice of States* – As earlier mentioned, it is not necessary to look at all States to find a new CIL rule.[244] The choice of States, nevertheless, is crucial for a degree of objectivity in the research. To this end, a choice of States was made based on two noncumulative factors:

1. The UN, using their Group of Governmental Experts mandate, has mentioned them as involved in the debate.[245]

2. Academic authors have identified them as being involved in the debate.[246]

---

[242] *Ibidem.*
[243] Danae Azaria, "Codification by interpretation: The International Law Commission as an interpreter of international law," *The European journal of international law*, no. 31 (2020): 171-200.
[244] See *supra* margin number 50.
[245] "Cyber Toolkit: Interactive Toolkit," UN, accessed May 17, 2024, https://cyberlaw.ccdcoe.org/wiki/Main_Page.
[246] Droege, "Get off My Cloud," 533–78, https://doi.org/10.1017/S1816383113000246; Sohail, "Fault Lines in the Application of International Humanitarian Law to Cyberwarfare," 1–13; Michael N. Schmitt, "Wired Warfare 3.0:

68 *Third factor* – The previously mentioned factors have presented a group of seventeen States which include three quite controversial ones, considering the topic: China, Russia, and Ukraine. However, to keep the research feasible and ensure that sufficient sources are available, a third factor has been implemented: only States with official written reports on the topic available (in a language that is understood by the author), are included. The reason behind this is threefold: first, the DCICIL mentions that official written State reports are (one of) the most important evidential elements for customary law. Second, since the research is done by one researcher within a limited timeframe, the third factor ensures the research's feasibility. Due to this third factor, China, Russia and Ukraine were left out.

69 *List of States* – Considering the previous paragraphs and the three factors, this results in the following group of States: Australia, Belgium, Brazil, Chile, Denmark, France, Finland, Germany, Israel, New Zealand, Norway, Romania, Switzerland, and the United States. Importantly, the author is aware that the list of States is not free of any issues. For example, there is no African State included in the choice of States. In addition, not only these States, but many others have allegedly faced cyberattacks[247], including for example South Africa and India.[248] The reason these States are not included in the research is merely the combination of the three factors used to select the States, and the limited timeframe of this master's thesis. The author therefore wants to mention that she understands the limited scope of her own research and is aware of the biases which arise out of the State selection.

Protecting the Civilian Population during Cyber Operations," *International Review of the Red Cross* 101, no. 910 (April 2019): 333–55, https://doi.org/10.1017/S1816383119000018; Geiß and Lahmann, "Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space," 381–99; McKenzie, "Cyber Operations against Civilian Data," 1165–92; Gül, "Changing Notion of Object and Targeting Data Under the Law of Armed Conflict".

[247] The notion 'allegedly' is used to refer to the fact that States often do not want to recognise that they have been the victim of a cyberattack. This can happen for various reasons, but one in particular is the fact that they do not want to bring under the attention of all States that their system is in some way vulnerable.

[248] "New research suggests Africa is being used as a 'testing ground' for nation state cyber warfare," Dark Reading, accessed May 1, 2024, https://www.darkreading.com/cybersecurity-operations/new-research-suggests-africa-is-being-used-as-a-testing-ground-for-nation-state-cyber-warfare; "State-sponsored cyberattacks against India went up by 278% between 2021 and September 2023: Report," The Wire, accessed May 1, 2024, https://thewire.in/tech/state-sponsored-cyber-attacks-against-india-went-up-by-278-between-2021-and-september-2023report#:~:text=New%20Delhi%3A%20State%2Dsponsored%20cyber,a%20new%20report%20has%20found.

70 *Scope of research* – Considering the three factors mentioned earlier, the researcher is left with fourteen relevant States. This still results in a large amount of practice to study. To ensure the feasibility of the research, the author has contacted cyber defence committees and governments to ensure that she will focus on the sources seen by the State itself as the most relevant ones.[249] An overview of these contacts can be found in annex 4.

71 *Two elements* – Considering the importance of both elements, some authors claim that *opinio juris* is of greater importance in "modern" CIL. They thus argue that the weight given to the practice may be reduced, depending on the circumstances.[250] How this should be measured exactly, is not clear. Michael WOOD states that depending on the circumstances, there can indeed be a difference in assessment of both constituent elements. He adds, however, that the underlying rule remains that both are necessary.[251] In this research, this means that if the *opinio juris* is explicitly pronounced on considering data an object, but there is relatively little evidence in State practice, then the combination could still be considered sufficient. In contrast, if the approach in State practice varies every time a new case arises or is the opposite of what a State says, this can be regarded as a lack of consistent practice.[252] Important is that the practice must not be 100 percent in conformity with the rule in question. State conduct inconsistent with the rule can be considered breaches as opposed to inconsistencies.[253] The practice must nevertheless be sufficiently widespread, representative, and consistent.[254]

72 *Primary sources* – Regarding the sources used as evidence, Niels PETERSEN has analysed the case law of the ICJ to find out which sources it pays particular attention to. He concluded that

---

[249] For an overview of these contacts, see *infra* annex 4.
[250] ILC, *Draft Conclusions*, conclusion 7, §2; Haljan, *Separating Powers*, 213-214; Ratner, "Sources of International Humanitarian Law and International Criminal Law: War/Crimes and the Limits of the Doctrine of Sources," 920; Robert Kolb, *Advanced Introduction to International Humanitarian Law* (Cheltenham: Edward Elgar Publishing, 2014), 73–74; *contra* Talmon, "Determining Customary International Law: The ICJ's Methodology between Induction, Deduction and Assertion,".
[251] Michael Wood, "The present position within the ILC on the topic "Identification of customary international law": in partial response to Sienho Yee, Report on the ILC Project on "Identification of Customary International Law," *Chinese Journal of International Law,* (2016): 3-15.
[252] Jing Zhi Wong, "Comparative Legal Methodology and Its Relation to the Identification of Customary International Law," SSRN Scholarly Paper, accessed March 22, 2024, https://papers.ssrn.com/abstract=3655195.
[253] North Sea Continental Shelf Cases; Nicaragua Case; ILC, *Draft Conclusions*, conclusion 2, 7, §2, and 9; La Haye, *War crimes in internal armed conflicts*, 55.
[254] ILC, *Draft Conclusions*, conclusion 8.

the ICJ refers to: treaties, whether the parties in a case before the ICJ have consented to the norm in question, precedents of the ICJ itself, and resolutions of international institutions, followed then by an analysis of the national practice.[255] This is contrary to the ILC which has explicitly demanded the evidence should come primarily out of national documents.[256] Given that the author's emerging custom argument focuses on national practice, this master's thesis is thus mostly in line with the preferred approach of the ILC.[257]

73 *National sources* – PETERSEN nevertheless further explains that the most used national sources invoked as evidence of CIL, are official statements and domestic court decisions.[258] An example of this is the *Jurisdictional Immunities* Case by the ICJ.[259] For this research, the official State reports and communications on how IHL principles should apply to cyber operations, consequently are of particular significance.[260] They present the primary source of *opinio juris* in this case. The primary sources for the second criterion consist of: the most important national court decisions, opinions on the activities of other States, comments made at the international level, and official State reports mentioning State's activities.[261] The latter source is thus used in the two separate evaluations. The ILC accepts this method, if the source is explicitly evaluated twice in two different lights.[262] To fulfil this requirement, they are divided into separate sub-questions. Regarding the State practice, the question looked at should for that purpose be: "what

---

[255] Niels Petersen, "The International Court of Justice and the Judicial Politics of Identifying Customary International Law," *European Journal of International Law* 28, no. 2 (May 2017): 368, https://doi.org/10.1093/ejil/chx024.
[256] ILC, *Draft Conclusions*, conclusion 3 and 4, §3.
[257] For an overview of the sources considered, see *infra* annex 5.
[258] Ammann, *Domestic Courts and the Interpretation of International Law,* 151; Petersen, "The International Court of Justice and the Judicial Politics of Identifying Customary International Law,"; Scoville, "Finding Customary International Law," 1908.
[259] *Jurisdictional Immunities of the State (Germany v Italy: Greece intervening)*, ICJ Reports 2012, 99, International Court of Justice (ICJ), 3 February 2012 (Jurisdictional Immunities Case); ILC, "The Role of Decisions of National Courts in the Case Law of International Courts and Tribunals of a Universal Character for the Purpose of the Determination of Customary International Law: Memorandum by the Secretariat", A/CN.4/691 (February 9, 2016).
[260] La Haye, *War crimes in internal armed conflicts*, 56; An overview of the relevant sources as well as the methods used to detect them, can be found in annex 3.
[261] ILC, *Draft Conclusions*, conclusion 12 and 13; Raphaël van Steenberghe, "Sources of International Humanitarian Law and International Criminal Law: Specific Features," 898.
[262] ILC, *Draft Conclusions*, conclusion 3, §2.

is the State doing?", whereas for *opinio juris*, this question changes into: "is the State doing this out of a feeling of obligation or out of something else, for example tradition?".[263]

74 *Scheme* – To not disregard the criticism on CIL-making entirely, the findings of this research are presented in a scheme, categorised as affirmative, negative, or inconsistent evidence of the author's emerging custom argument.[264] That way, it presents a clear overview of State's activities, understands the criticism, but does not overthrow the traditional approach of the ICJ, which is still considered as the most influential one on CIL. Armed with this information, the analysis of States' activities can begin.

[263] *Ibidem.*
[264] See *infra* annex 6.

CHAPTER II: EVALUATION OF BOTH ELEMENTS

75 *Overview* – This chapter contains an in-depth discussion of the results found during the analysis regarding the emerging custom argument. The sources of the fourteen previously mentioned States were analysed thoroughly and presented in annex 5. The smaller scheme in annex 6 summarises the most important findings of annex 5. The text in this chapter is meant to be read alongside these two annexes.

1. Considering data an object under the principle of distinction

76 *Analysis* – As mentioned in the previous chapter, the first step is to look at the State practice: does State 1 do X (with X= a specific action or an omission)?[265] In this research, the question is thus put as follows: does State 1 consider data to be an object in its practice? This same question is then asked for every of the fourteen States. The second step is to look at the *opinio juris* of all fourteen States: does State 1 believe that doing X is the law?[266] In this research, the *opinio juris* is mostly looked at through official statements in which States explicitly mention their opinion on cyber warfare. Do they explicitly mention a legal obligation to consider data an object under the principle of distinction? These two tests brought up the following results.

77 *Traditional approach* – As the schemes in annex 5 and 6 present, three States explicitly hold on to the theory upheld in TM 2.0 that an object under IHL must be visible and tangible: Denmark, Israel, and the United States.[267] Only when an attack on data results in physical effects as well, the principle of distinction applies.[268] Israel has already been suspected of attacking a civilian dataset of Iran in 2020.[269] This potentially is a type A example of their State

---

[265] See *supra* margin number 71.
[266] *Ibidem.*
[267] Denmark, *National position: contribution to the United Nations Group of Governmental Experts on Cyber* (July 2013); "Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations (26 January 2021)," Israel, accessed May 1, 2024, https://digital-commons.usnwc.edu/ils/vol97/iss1/21; *Stockx Customer Data Security Breach Litigation*, United States Federal Court of Appeals for the Sixth Circuit, 2 December 2021. See *infra* annex 5 and 6.
[268] Norway also referred to these secondary physical effects in its first statement. It nevertheless later on emphasised the potential effects an attack on civilian data could have. Therefore, it is considered affirmative of the effects-approach.
[269] *Official statement after cyberattack on Israel's water facilities*, Israel, April, 25, 2020.

practice disagreeing with considering data an object under the principle of distinction.[270] The United States' practice too has made clear that an attack on data as such, without further physical consequences but merely, for example, economic damage, is insufficient.[271]

78 *Lack of clarification* – Three States, Brazil, Chile, and Switzerland, neither agree nor disagree with the reasoning that data is considered an object.[272] In general, Chile and Switzerland accept IHL applying in cyberspace, as well as the principle of distinction, but they do not specify whether this means that data is an object.[273] As is mentioned in annex 6, Brazil mentions it fears a copy paste of IHL as it currently stands in cyberspace: unqualified transfers of IHL would cement "*a Western-biased status quo*".[274] This could suggest support by Brazil for the consideration of data as an object, because the traditional IHL approach requires an object to be tangible. Switzerland mentions, in its most recent acts, an increasing concern for the potential effects in case civilian data is not considered a civilian object under the principle of distinction.[275]

79 *Modern approach* – Only one State's activities, in both court decisions and official statements, confirm in total that it does consider data an object: Belgium.[276] It is the only State which agrees with the statement as such, but in recent years has started explaining that it does so because of the potential effects an attack on civilian data can have. This evolution is important because the

---

[270] *Ibidem.*
[271] Stockx Customer Data Security Breach Litigation.
[272] "National position: contribution to the UN GGE," Brazil, accessed May 1, 2024, https://cyberlaw.ccdcoe.org/wiki/National_position_of_Brazil_(2021); "Chile's Cyber Security Strategy 2017-2022," Chile, accessed May 1, 2024, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Chile_NCSP%20%28ENG%29.pdf; "National position: contribution to the UN GGE," Switzerland, accessed May 1, 2024,https://ceipfiles.s3.amazonaws.com/pdf/CyberNorms/UNGGE/Position+Paper+on+Switzerland's+Participation+in+the+2019-2020+UN+Open-Ended+Working+Group+on+"Developments+in+the+Field+of+Information+and+Telecommunications+in+the+Context+of+International+Security"+and+the+2019-2021+UN+Group+of+Gov.pdf.
[273] Chile, "Chile's Cyber Security Strategy 2017-2022"; Switzerland, "National position".
[274] Brazil, *Cyber Security Strategy* (8 august 2023).
[275] "National position on public international law in cyberspace," Switzerland, accessed May 1, 2024, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/20230308_Switzerland_submission_OEWG_international_law_as_delivered.pdf.
[276] Court of Cassation, *AR P.10.1094.F*, 5 January 2011; Court of Cassation, *AR P.16.0048.N/1*, 24 January 2017; Criminal Court of Dendermonde, *No. 2007/81*, 14 May 2007; Criminal Court of Hasselt, Fifteenth Chamber, 21 January 2004; Belgium, *Cyber Security Strategy 2021-2025* (1 May 2021).

remaining seven States have not shown evidence of considering data an object as such. Instead, they focus on the effects it could have not to protect it under the principle of distinction.

80 *State practice* – Overall, as can be seen in the scheme in annex 6, the search for State practice has shown various results.[277] A majority of State activities affirms that civilian data is not a lawful target under the principle of distinction. Yet, not because of its status as 'civilian object' *per se*. This reasoning is further explained in the following part. Important is that this does not mean the end for the research. As mentioned in the previous chapter, if the *opinio juris* is overwhelmingly affirmative, then the emerging custom argument made by the authors could still be found to be correct.[278]

81 *Opinio juris* – For *opinio juris*, it is important to consider whether the approach taken by States is backed up by a belief that they are legally obliged to act in such ways. Looking at the scheme in annex 6, most of the *opinio juris* aligns with the actions made by the fourteen States.[279] That is to say, Denmark, Israel, and the United States believe that an object as envisaged under IHL can only be tangible, thereby leaving out data.[280] Israel, however, made a statement that they believe this is true considering the law as it currently stands: they leave a door open for the future.[281] This opinion makes Israel's disagreement seem less harsh than that from Denmark and the United States.

82 *Potential effects* – Regarding the three States who lacked explicit practice on the matter: Brazil's beliefs are equally unclear, but Chile and Switzerland seem to uphold a similar approach in their *opinio juris* as some other States.[282] States which were, as presented in annex 5, more concerned with the potential effects of not allowing data to fall under the principle,

---

[277] See *infra* annex 6.
[278] See *supra* margin number 71.
[279] See *infra* annex 6.
[280] See *infra* annex 6.
[281] "Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations".
[282] "State report: IL applicable to cyberspace," Chile, accessed May 1, 2024, https://www.oas.org/en/sla/iajc/docs/CJI-doc_671-22_rev2_corr1_ENG.pdf; "National position on public international law in cyberspace," Switzerland, March, 18, 2021.

than the actual status of data as an object.[283] It is joined in this opinion by Australia, Belgium (in its most recent statements), Finland, France, Germany, New Zealand, Norway, and Romania.[284] Belgium, however, also maintains a strong belief in considering data an object as such under the principle of distinction.[285] There is only one State in annex 6 for which the State practice and the *opinio juris* does not totally align: France.[286] In its official statements, France puts out strong affirmative opinions on the subject, considering 'content data' (including governmental, banking-, and medical data) an object.[287] In its actual State practice nonetheless, this opinion is not upheld.[288]

83 *Summary* – Overall, the result of this analysis is that, referring to a broad range of official statements, military manuals, court decisions, and responses to real-life cyberattacks, there is currently no general agreement on considering data an object under the principle of distinction. However, this does not mean that a general reasoning on the subject matter does not seem to arise. As TALMON mentioned in his theory around finding customary law, one must seek generalities amongst specificities, a reoccurring element.[289] That reoccurring element, is the continuing mention of the potential effects an attack on civilian data might have.

---

[283] See *infra* annex 5.
[284] *Australian Securities and Investments Commission / RI Advice Group Pty Ltd*, Federal Court of Australia 2022; Belgium, "Cyber Security Strategy 2021-2025,"; "National position: contribution to the UN GGE," Finland, accessed May 1, 2024, https://cyberlaw.ccdcoe.org/wiki/National_position_of_Finland_(2020); French Ministry of Defence, *Report international law applicable to operations in cyberspace* (12 November 2018); "National position on public international law in cyberspace," Germany, accessed May 1, 2024, https://www.justsecurity.org/75242/germanys-positions-on-international-law-in-cyberspace/; "National position: contribution to the UN GGE," New Zealand, accessed May 1, 2024, https://ceipfiles.s3.amazonaws.com/pdf/CyberNorms/UNGGE/Position+Paper+on+New+Zealand's+Participation+in+the+February+2020+Session+of+the+2019-2020+Open-Ended+Working+Group+on+Developments+in+the+Field+of+Information+and+Telecommunications+in+the+Context+of+International+Security+.pdf; Norwegian Ministry of Defence, *Manual on the law of armed conflict* (19 March 2012); "Voluntary national contribution on the subject of how IL applies to the use of information and communications technologies by Romania submitted in the Group of Governmental Experts," Romania, accessed May 1, 2024, https://cyberlaw.ccdcoe.org/wiki/National_position_of_Romania_(2021).
[285] Belgium, "Cyber Security Strategy 2021-2025".
[286] See *infra* annex 6.
[287] See *infra* annex 5.
[288] "Statement: Open-Ended Working Group on IL applied to operations in cyberspace," France, July, 14, 2021; Court of Appeal of Lyon, Eight Chamber, *N° 20/07493*, 10 November 2021.
[289] See *supra* margin number 63.

2. Protecting data as an object under the principle of distinction

84 *Not an object* – Most of the States did not affirm that they consider data an object under the principle of distinction.[290] Yet, they are aware that if data did not fall under the principle, certain actions with dramatic consequences for civilians would be fair game. As a result, these States put two and two together and seem to agree that, for now, the law does not consider data an object. However, considering the potential consequences, it should be and is protected as one.

85 *Nicaragua Case* – The idea of looking at effects for deciding what the law should be is not new in IL. In the *Nicaragua* Case, the ICJ mentioned that when determining which act can be treated as an armed attack, the scale and effects of such acts must be considered.[291] Hence, the notion 'scale and effects approach': 'scale and effects' means all relevant quantitative and qualitative factors that must be analysed when an act is considered an armed attack.[292]

86 *Scale and effects approach in TM 2.0* – As mentioned in the beginning of this master's thesis, the question on data is not the only unresolved discussion in this subject matter. A similar debate exists regarding the notion of the 'use of force'. Can the threshold for an armed attack be reached when a cyberattack causes only nonphysical effects, for example economic ones? The TM 2.0 answered this question affirmatively by referring to the scale and effects approach in the *Nicaragua* Case.[293] TM 2.0 suggested that "*a cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of use of force*".[294] Similar to the *Nicaragua* Case, 'scale and effects' in TM 2.0 entails all quantitative and qualitative factors necessary for determining whether a cyber operation is considered 'use of force'.[295]

---

[290] The States I refer to here include: Australia, Belgium, Chile, Finland, France, Germany, New Zealand, Norway, Romania, and Switzerland.
[291] Nicaragua Case, §195, 103-104.
[292] *Ibidem.*
[293] Schmitt, *Tallinn Manual 2.0*, "Rule 69", 330-331.
[294] Schmitt, *Tallinn Manual 2.0*, "Rule 69", 330-331.
[295] Michael N. Schmitt, "Israel's Cautious Perspective on International Law in Cyberspace: Part II (jus ad bellum and jus in bello)," EJIL Talk, accessed April 15, 2024, https://www.ejiltalk.org/israels-cautious-perspective-on-international-law-in-cyberspace-part-ii-jus-ad-bellum-and-jus-in-bello/.

87 *Scale and effects on data* – For the question of considering data an object or not, the scale and effects approach was not suggested by the experts of TM 2.0. They only described it as being linked to the notion of 'attack'. The evidence of State practice and *opinio juris* by the relevant States seems to approach the question in a similar way as the 'attack'- debate. This similarity can also be seen as a logical consequence from a pragmatic perspective: when one assesses whether a particular cyberattack reaches the threshold of an attack under IHL, it could use this scale and effects approach. Next, when examining whether the attack respects the principle of distinction, it could then use the same approach. As a result of applying the scale and effects approach to the notion of 'object', the relevant States do not consider data an object as such. However, due to the potential scale and effects leaving an attack on civilian data unprotected brought the States to protect civilian data as if it was a civilian object under the principle of distinction.

88 *Threshold* – The States do not currently suggest a certain threshold that must be met for data to be protected. Considering the previous mentioned pragmatic argument of having the same test applied to both the notion of 'attack' and to 'object', it would be useful if this is a similar threshold. Applying a similar threshold to the scale and effects approach on the 'object' notion could be: would a non-cyber operation entail similar results for e.g. the economy or the education system? That way, the non-physical effects of an attack could be taken into account when assessing whether an attack respects the principle of distinction, without saying that data is an object.

3. Critical infrastructures

89 *Infrastructures* – Another generality amongst specificities found in the analysis consists of the need for additional protection for 'critical infrastructures'. Many States have argued specific concerns for the datasets linked to a particular function in their society. In general, the reoccurring ones were the following: education, medical, finance, telecom, water and food

facilities, energy, government, and research.[296] No State has, to this day, clearly defined the notion 'critical infrastructure'. The author of this thesis consequently presents her own view.

90 *Author's view* – Looking back into the wording used by States and considering that the ICRC's report on the principle of distinction concludes that this notion "*has no legal importance"*, the author believes that 'critical infrastructure' does not entail a legal term.[297] Rather, it is a non-legal descriptor used by States to indicate that something is of crucial functioning to society and consequently to civilians. One could criticise this view by arguing that this would result in varying descriptions of what a critical infrastructure is. However, as presented in annex 5, States generally refer to the same functions. As a result, the author does not believe that using the non-legal term 'critical infrastructure' is an issue. Instead, the author's concern relies more on what is linked to these critical infrastructures: the need for 'additional protection'.

91 *Protection* –What the above-mentioned 'additional protection' should precisely consist of is not explained by any of the States. Regarding medical datasets, it was already clarified that these receive protection under a specific regime that obliges States to protect it under all circumstances.[298] The ICRC has also mentioned that electricity and water facilities must never be attacked.[299] The reason is that a dual-use object may only be targeted when (1) it makes an effective contribution to a military action and (2) it offers a definite military advantage.[300] Do the State's opinions entail that for these infrastructures, the datasets must always be considered civilian, because of their detrimental effects on society? Or, going even further, is data, as part of these infrastructures, always considered an object? Or does 'additional protection' merely mean an obligation towards the State itself to ensure that these assets are protected? These questions have remained unanswered in the analysis. The author of this thesis argues that the

---

[296] Australia, *Cyber threats report 2022-2023* (14 November 2023); Brazil, *Comments on the draft report of the UN OEWG* (8 April 2020); Danish Government, *Danish cyber and information security strategy* (1 May 2018); Israel, *Official Statement on the application of International Law to cyberspace* (25 October 2021); Norway, *National position: contribution to the UN GGE* (13 July 2021); Romanian Ministry of National Defence, *The military strategy of Romania* (1 January 2016); Switzerland, *Report on the Security Policy* (23 June 2010).
[297] ICRC, "The principle distinction". See *infra* annex 5.
[298] Art. 12 AP I; "The Principle of Distinction," ICRC, accessed May 1, 2024, https://www.icrc.org/sites/default/files/wysiwyg/war-and-law/03_distinction-0.pdf; see *supra* margin number 22.
[299] ICRC, "The principle distinction".
[300] *Ibidem.*

phrasing of the States hints towards 'additional protection' being a type of *ex ante*-control over critical elements of society. However, it remains unclear on which State the burden of additional protection is intended to fall: the perpetrating State putting out a cyberattack, or the victim State? In addition, could the additional protection be similar to the obligations necessary for attacking a dual-use object?[301]

4. Interim conclusion: were the authors right?

92 *Resume* – The investigation of the official statements all started by a disputed statement made against the majority of experts of TM 2.0. In general, they presented three arguments. One of the arguments was that there is a customary rule emerging considering data as an object. After the analysis of State's activities, does the author of this thesis agree?

93 *No agreement* – There appears to be no general agreement on the nature of data. However, States do realise that leaving whole civilian datasets without protection would be detrimental to civilians, certainly seeing the potential effects an attack can have on society. As a result, their statements generally adopt the 'scale and effects approach': data is not as such considered an object, but because of the potential scale and effects for civilians that an attack on them can have, it is still protected under the principle of distinction. This description as a result may be taken to refer emerging CIL. Consequently, the authors' statement was partially true.

94 *Critical infrastructures* – In addition, the results have shown States' particular interests in critical infrastructures of all kinds and the need for their additional protection. As mentioned, States do not further explain what is meant by this 'additional protection'. However, their concern for critical infrastructures has clearly influenced their reasoning on the status of data under IHL. This is shown in the numerous references the States make to this notion, as presented in annex 5.

---

[301] See *infra* margin number 98.

Chapter III: Scenarios

95 *Relevance* – The findings described in the previous chapter seem quite theoretical. They do, however, have consequences in practice as well. The fact that certain data is not generally protected, but only when a certain threshold is met, obviously makes one wonder what that threshold will look like in practice. For that reason, this chapter investigates five fictitious scenarios, provided by Robin GEISS and Henning LAHMANN.[302] The author of this thesis has linked the fictitious scenarios to real-life examples of cyberattacks.[303] These attacks have remained relatively little studied from a legal perspective. Linking the attacks to the findings of the States' activities analysis can give a greater understanding of them. The real-life examples show that although the first scenarios are fictional, reality is not far off. Because this thesis discusses only *jus in bello*, it will assume that the real-life examples all take place in an armed conflict.

96 *Annex 1* – In the following paragraphs, each fictitious scenario and the real-life example linked to it is briefly summarised before applying the TM 2.0 approach and the 'general approach of the studied States' to them. For structural purposes, an in-depth description of the facts of the scenarios and the real-life examples can be found in annex 1. The author advises to read the descriptions in annex 1 first to thoroughly understand the analysis presented in this chapter.

97 *Figure* – It is useful to repeat in a concise manner the difference between the approach adopted in the TM 2.0 and the 'general approach of the studied States' against various types of cyber conduct.[304] The following figure presents what both perspectives believe is protected under the notion of 'civilian object' in line with the principle of distinction.

---

[302] Geiß and Lahmann, "Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space," 381–399.
[303] See *infra* annex 1.
[304] The notion 'general approach of the studied States' refers to the analysis of both *opinio juris* and State practice, which presented evidence of a general use of the scale and effects approach by most States.

Potential target	TM 2.0 approach	General approach of the studied States
Cyber infrastructure	X (object)	X
Data, through which also the infrastructure	X (physical effect)	X
Data as such		X (if the scale and effects approach is fulfilled)

Figure 2: cyber infrastructure protected in theory under TM 2.0 and the general approach of the studied States

98 *Dual use* – Before diving into the scenarios and the real-life examples, the notion of 'dual-use objects' under IHL must be elaborated on. Dual-use objects are objects used for both civilian and military purposes at the same time.[305] Examples are the use of the same satellite or electricity grid. The dual use entails that when attacked, it is inevitable that civilian damage will occur. To minimise such damage, an attack on a dual-use object can only take place when it fulfils the two conditions all military objectives must fulfil.[306] These conditions entail that the attack must make an effective contribution to the military action and must offer a definite military advantage.[307] Because of the interconnectivity which characterises cyberspace, the above notion and conditions must be remembered when discussing the different attacks.

99 *First scenario* – The first scenario consists of a ransomware attack against the patient data of a medical facility.[308] No physical infrastructure was damaged due to this attack, but certain operations had to be postponed. Following the approach upheld in TM 2.0, this attack would not be in line with IHL. That is to say, as the data are part of a medical facility, it receives protection under a specific regime.[309] It can thus not be lawfully targeted.

[305] ICRC, "The principle distinction".
[306] ICRC, "The principle distinction".
[307] *Ibidem.*
[308] See *infra* annex 1.
[309] See *supra* margin number 22.

The real-life example, as mentioned in annex 1, is the Springhill Medical Center attack.[310] The medical center had to shut down its entire computer system because it refused to pay the ransom. As a result, all health records were inaccessible and the medical staff had to resort to phone communication, leaving certain monitors unmanned. Hence, no one noticed the umbilical cord around a child's neck during delivery. Similar to the abovementioned approach, the real-life example of the Springhill Medical Center attack, if it happened in an armed conflict, would also be treated as an unlawful attack.[311] Would the attack, for example, have occurred against online student files in a school, this would not have violated the principle of distinction as put forward by TM 2.0. Civilian data is not a civilian object.

Taking now the general approach of the studied States, the results would be different. As it focuses on potential effects (e.g. here the potential complications for patients), it would conclude that the data, even if not part of a medical facility, constitutes an unlawful target. Following this approach, the attack on the Springhill Medical Center certainly was unlawful and violated the principle of distinction, should it have occurred during an armed conflict.

100 *Second scenario* – The second scenario can be resolved in a similar way as the first one.[312] According to the TM 2.0 approach this would constitute a lawful attack if the conditions for an attack on a dual-use object are respected. This is because, again, the target entails pure data and the consequences are merely economic and financial. However, no physical (tangible) effect is found. Consequently, the real-life attack on the Colonial Pipeline would be considered lawful as well.[313] In this attack, the data of one of the largest fuel suppliers in the USA was stolen, which led to the preventive closure of the distributive network. Due to a panic buyout of fuel, there was a shortage which increased the prices significantly.[314]

---

[310] See *infra* annex 1.
[311] "Cyber Toolkit: Springhill Medical Center ransomware attack (2019)", UN, accessed November 2, 2023, https://cyberlaw.ccdcoe.org/wiki/Springhill_Medical_Center_ransomware_attack_(2019).
[312] See *infra* annex 1.
[313] "Cyber Toolkit: Interactive Toolkit," UN, accessed May 17, 2024, https://cyberlaw.ccdcoe.org/wiki/Main_Page.
[314] See *infra* annex 1.

The general approach of the studied States as found in the analysis would, contrary to the TM 2.0, focus on the detrimental effect on the stock market and the employment sector. As a result, it would find the target unlawful, just like it would the real-life attack on the Colonial Pipeline. Regarding that real-life attack, the analysis explicitly mentioned a need for protection of critical infrastructure, such as the provision of fuel. It currently remains unclear however, what States mean by that. Potentially, this explicit mention could be an additional reason for considering the attack in violation of the principle of distinction.

101 *Third scenario* – The third scenario consists of a cyberattack against the data of a water treatment facility.[315] The employees shut down the facility with water shortages as a result. For the TM 2.0 approach, this might prove a tricky scenario. The attack again targets an intangible set of data. There is no physical destruction of the system itself: the employees shut it down. Yet, the water shortages can be treated as a secondary physical effect. In addition, the ICRC argues that a water facility cannot be targeted.[316] The Committee said so, because a water facility is a dual-use object. Consequently, it must respect the two conditions of effective contribution and definite military advantage.[317] Considering this commentary by the ICRC and the physical effect of the water shortage, the TM 2.0 would find this an unlawful attack against the water facilities' data. Similarly, the general approach of the studied States would come to the same conclusion. It would thereto use a different reasoning, however. Namely that the attack has effects for civilians due to the water shortage. The fact that the water treatment facility also constitutes a critical infrastructure potentially adds to the case, even though 'critical infrastructure' is not a legal notion.

A real-life example of an attack against a dataset which led to the denial of service of a critical infrastructure is NotPetya.[318] The cyberattack resulted in a severe economic loss and the shutdown of Ukraine's Chernobyl Nuclear Power Plant. Both TM 2.0 as well as the general approach of the studied States would find this target unlawful because of the physical

---

[315] See *infra* annex 1.
[316] See *supra* margin number 91.
[317] *Ibidem.*
[318] "Cyber Toolkit: NotPetya (2017)", UN, accessed November 2, 2023. https://cyberlaw.ccdcoe.org/wiki/NotPetya_(2017).

consequences for Chernobyl. If there merely had been economic loss, then only the studied States practice would have considered this a violation of the principle of distinction.

102 *Fourth scenario* – The leakage of data by a hacker group would not entail an unlawful target under the approach upheld in TM 2.0.[319] The general approach of the studied States would potentially conclude differently because of the detrimental effect on civilians of the leakage of a large amount of social security numbers. At the same time, the exposure of certain employees' sexual orientation would probably not be sufficient to fulfil the quantitative factor of the scale and effects approach.

A real-life example of data leakage is the Sony Pictures Entertainment Attack.[320] As described in annex 1, Sony's internal network and database were hacked which resulted in the leakage of both personal information and unpublished scripts.[321] Similar to the first scenario, the conclusion of TM 2.0 would not be to consider such leakage unlawful during armed conflict. Neither would the general approach of the studied States consider this a violation of the principle of distinction. The States would conclude so because, even though there are economic effects due to the scripts' leakage, these are insufficient to reach the quantitative threshold of the scale and effects approach.[322]

103 *Fifth scenario* – The fifth scenario consists of data theft used for blackmailing.[323] Taking a similar approach as in the analysis of the previous scenario, the TM 2.0 approach would not consider the mere theft of location data and call records to constitute an unlawful target.[324] That being said, because a phone and internet provider consists again of a dual-use object, the TM 2.0 approach would only decide so when the two previously discussed conditions are met. The additional factor of blackmailing is considered irrelevant: the UN concluded certain types of

---

[319] See *infra* annex 1.
[320] "Cyber Toolkit: Sony Pictures Entertainment Attack (2014)", UN, accessed November 2, 2023. https://cyberlaw.ccdcoe.org/wiki/Sony_Pictures_Entertainment_attack_(2014).
[321] See *infra* annex 1.
[322] *Ibidem.*
[323] See *infra* annex 1.
[324] See *infra* annex 1.

coercion do not entail 'use of force'.[325] These include both economic and political coercion. In the real-life example of the Office of Personnel Management, in which sensitive information of approximately 21.5 million individuals was stolen, the TM 2.0 approach would come to a similar decision.[326]

The general approach of the studied States would conclude otherwise both in the fictitious case and in the real-life example. In both scenarios, the unlimited amount of personal data stolen would result in the attack being considered unlawful. The blackmailing factor in the fictitious case would be disregarded.[327] In contrast, the identity theft of numerous employees in the real-life example would be a relevant factor in its decision.[328]

104 *Summary* – The analysis of the five scenarios and real-life examples presents the following results when transferred to the table below:

[325] UN GAOR Special Comm. on Friendly Relations, UN Doc. A/AC.125/SR.110 to 114: 1970; Schmitt, *Tallinn Manual 2.0*, "Rule 69", 331.
[326] "Cyber Toolkit: Office of Personnel Management data breach (2015)", UN, accessed November 2, 2023. https://cyberlaw.ccdcoe.org/wiki/Office_of_Personnel_Management_data_breach_(2015).
[327] See *infra* annex 1.
[328] "Cyber Toolkit: Office of Personnel Management data breach (2015)", UN, accessed November 2, 2023. https://cyberlaw.ccdcoe.org/wiki/Office_of_Personnel_Management_data_breach_(2015).

Scenarios	TM 2.0 approach	General approach of the studied States
Medical facility	Unlawful: special regime	Unlawful: special regime and scale and effects approach
Springhill Medical Center Attack	Unlawful: special regime	Unlawful: special regime and scale and effects approach
Financial damage	Lawful	Unlawful: scale and effects approach
Colonial Pipeline Attack	Lawful	Unlawful: scale and effects approach and critical infrastructure
Essential facilities	Unlawful: dual-use object conditions are not met	Unlawful: scale and effects approach and critical infrastructure
NotPetya	Unlawful: dual-use object conditions are not met	Unlawful: scale and effects approach and critical infrastructure
Data leakage	Lawful	Unlawful: scale and effects approach
Sony Pictures Entertainment Attack	Lawful	Lawful
Data theft	Lawful	Unlawful: scale and effects approach
Office of Personnel Management data breach	Lawful	Unlawful: scale and effects approach

Figure 3: cyber infrastructure protected in practice under TM 2.0 and the general approach of the studied States

105 *Conclusion* – In conclusion, in nine out of thirty cases, the TM 2.0 approach and the general approach of the studied States would uphold the same outcome. Even in these nine cases, however, their reasoning to come to this result would be significantly different. In the other 22 cases, they would uphold a different conclusion. The reasoning flowing from the TM 2.0 seems to leave much more data out in the open than what States envisage, and what thus flows from their practice and *opinio juris*. As a result, it seems these authors of the emerging custom argument who criticised the approach upheld in TM 2.0 made a half-true statement: data is not, by States following an emerging custom, considered an object, but it is protected as one under the principle of distinction.

CONCLUSION

106 *Main topic* – The focus of this master's thesis rested on the interpretation of IHL's principle of distinction in relation to cyber operations. The current approach in TM 2.0, that data is not considered an object, was criticised for leaving too many cyber operations against civilian data without a sufficient level of protection in IHL. Scholars' most important argument for criticising TM 2.0, however, was that there is a custom emerging considering data an object. The thesis referred to this as 'the emerging custom argument'. To evaluate the truthfulness of this argument, the master's thesis analysed the relevant activities of fourteen States.

107 *Part one* – Before doing so, the first part of the thesis compared the relevance of a custom on cyber conduct in IHL with the effects of other sources under art. 38 ICJ Statute. These included treaty provisions, general principles, and non-binding sources of IL. The comparison presented CIL as the most desirable source to have in the context of cyber warfare and IHL. As a result, the veracity of the emerging custom argument increased significantly in importance.

108 *Part two* – The assessment of the emerging custom argument brought up the following results. First, the evidence found is inconclusive on whether data is considered an object under the principle of distinction. The analysis, however, presented that States nevertheless protect it as one. The author of the thesis argued that this is an example of the scale and effects approach, originally defined by the ICJ in the *Nicaragua* Case. In this context, the author defined it as the following: the threshold is met when the scale and effects of a cyberattack have similar consequences, for instance for the economy, as the scale and effects of a non-cyber operation. As a result, the emerging custom argument was a partially true one: with sufficiently severe consequences, even though civilian data is not a civilian object, it is protected as one. To examine what this threshold precisely means, the thesis verified the results of the analysis through hypothetical scenarios and real-life examples of cyberattacks. The thesis compared the results to the approach of TM 2.0. This comparison showed that TM 2.0 leaves much more data unprotected than the States' activities aim for in both State practice and *opinio juris*. It can therefore be concluded from the assessment that the current approach in TM 2.0 was rightly criticised. A reinterpretation in the upcoming 'Tallinn Manual 3.0', with additional consideration of the potential large-scale impact on society is thus highly desirable.

109 *Limitations* – Equally important to presenting the result of the analysis is acknowledging the limits of the research. These limits, however, provide at the same time an opportunity to designate possible directions for further research. First, the thesis was written in a limited timeframe, which had an impact on the choice of States for the analysis. Based on three criteria, a preselection of seventeen States was made. Only fourteen States made it to the final selection, given that they had at least one official statement published in language that is comprehensible for the author. This still resulted in a significant group. Even so, the selection has its limits from a geographical representation perspective.[329] An in-depth analysis of the activities of non-Western States is necessary to assess whether the current findings are applicable to a larger group of States. Second, the thesis has the *jus in bello* as a legal framework: it presumes that the cyber operations in question reached a level defined as an 'act of force'. Even though TM 2.0 endorses this approach, it must be mentioned that it is not entirely clear yet when one can speak of 'use of force' regarding a cyberattack. Further research is crucial on both *jus in bello* and cyber operations that do not reach the threshold of an armed conflict. For example, can the latter operations trigger international liability for damage? Third and final, the results of the analysis presented merely 'the tip of the iceberg'. States might not want to acknowledge that they have been the victim and/or the perpetrators of a cyberattack. Potentially, there are many more States' activities than the ones accessible to the author to analyse. Linked to the need for research on operations outside of *jus in bello*, there is an equally important need to seek a solution for this issue of attribution and lack of transparency.

110 *Future* – The easiest conclusion to draw from this thesis is the following: cyber warfare will not leave. On the contrary, considering the recent conflict between Russia and Ukraine, the war in Gaza, and States being increasingly interconnected through cyberspace, it will only gain in importance and, unfortunately, usage. Research regarding all aspects of cyber warfare is crucial to increase both the protection of civilian data in cyberspace, as well as the legal certainty around the consequences of such operations. Take, for example, the requirement of 'additional protection for critical infrastructures' mentioned by States: what does it precisely mean? Or

[329] For example, Senegal and Colombia have presented a cross regional statement on cyber warfare in March 2024 according to the ICRC: "Focus on cyber operations that cause physical damage is not enough," Statement by the ICRC, https://www.icrc.org/en/oewg-cyber-new-statement.

what about countermeasures? Shall one resort to a cyberattack when it has been the victim of one or may it also use conventional warfare? And what about a regime of cyber war crimes? These questions are important for society and remain unanswered today. This thesis aimed to present a first stepping stone for further research on the subject. As a result, the ICRC's Study on Customary International Humanitarian Law expresses the thesis' intentions in the following quote: *"may it be read, discussed, and commented on."*[330]

[330] Jean-Marie Henckaerts and Louise Doswald-Beck, *ICRC: Customary International Humanitarian Law: Volume I: Rules* (Cambridge: Cambridge University Press, 2009), xxiii.

BIBLIOGRAPHY

LEGISLATION (including reports, guidelines, and other sources)

1. Binding legislation: international level

Art. 92 United Nations Charter, 26 June 1945.

Art. 38 Statute of the International Court of Justice, 18 April 1946 (ICJ Statute).

Art. 3 Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, 12 August 1949 Geneva Convention (I).

Art. 12, 48, and 52(2) Protocol Additional to the Geneva conventions, 12 August 1949 (AP I).

Art. 26 and 53 Vienna Convention on the Law of Treaties, 23 May 1969 (VCLT).

2. Binding legislation: national level

§1. Australia

Section 476-478, Criminal Code concerning computer offences.

3. Reports, guidelines, and other sources: international level

United Nations. "UN GAOR Special Comm. on Friendly Relations." UN Doc. A/AC.125/SR.110 to 114 (1970).

International Committee of the Red Cross. "Commentary 8 June 1977 on the Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I)." Accessed March 22, 2024. https://ihl-databases.icrc.org/en/ihl-treaties/api-1977.

International Committee of the Red Cross. "Study on Customary International Humanitarian Law: A Contribution to the Understanding and Respect for the Rule of Law in Armed Conflict." *International Review of the Red Cross,* no. 87 (2005): 175-212.

United Nations General Assembly, Sixth Committee. *UN Doc. A/C.6/68/SR.17* (8 November 2013).

United Nations Cyber Toolkit. "Sony Pictures Entertainment Attack (2014)." Accessed November 2, 2023. https://cyberlaw.ccdcoe.org/wiki/Sony_Pictures_Entertainment_attack_(2014).

United Nations Cyber Toolkit. "Office of Personnel Management data breach (2015)." Accessed November 2, 2023. https://cyberlaw.ccdcoe.org/wiki/Office_of_Personnel_Management_data_breach_(2015)

International Law Commission. "The Role of Decisions of National Courts in the Case Law of International Courts and Tribunals of a Universal Character for the Purpose of the Determination of Customary International Law: Memorandum by the Secretariat." *A/CN.4/691*, (February 9, 2016).

International Law Commission. "ILC Report 2016." Accessed October 3, 2023. https://legal.un.org/ilc/reports/2016/.

United Nations Cyber Toolkit. "Notpetya (2017)." Accessed March 20, 2024. https://cyberlaw.ccdcoe.org/wiki/NotPetya_(2017)#:~:text=The%20NotPetya%20malware%20was%20spread,and%20repurposed%20by%20the%20GRU.

International Law Commission. *Draft Conclusions on identification of customary international law, with commentaries* (2018).

United Nations Cyber Toolkit. "Springhill Medical Center ransomware attack (2019)." Accessed November 2, 2023. https://cyberlaw.ccdcoe.org/wiki/Springhill_Medical_Center_ransomware_attack_(2019).

International Committee of the Red Cross. "ICRC Report 2020." Accessed March 20, 2024. https://www.icrc.org/en/document/annual-report-2020.

International Committee of the Red Cross. "The Principle of Distinction, March 2023." Accessed May 1, 2024. https://www.icrc.org/sites/default/files/wysiwyg/war-and-law/03_distinction-0.pdf.

International Committee of the Red Cross Global Advisory Board on Digital Threats During Armed Conflicts. "Protecting civilians against digital threats during armed conflict: recommendations to States, belligerents, tech companies, and humanitarian organizations." Accessed October 25, 2023. https://www.icrc.org/en/publication/473501-protecting-civilians-against-digital-threats-during-armed-conflict.

United Nations Cyber Toolkit. "Scenario 12: Cyber operations against computer data." Accessed December 19, 2023. https://cyberlaw.ccdcoe.org/wiki/Scenario_12:_Cyber_operations_against_computer_data#:~:text=The%20ICRC%20has%20highlighted%20medical,essential%20component%20of%20digitalized%20societies%27.

United Nations Cyber Toolkit. "Scenario 22: Cyber methods of warfare." Accessed December 19, 2023. https://cyberlaw.ccdcoe.org/wiki/Scenario_22:_Cyber_methods_of_warfare.

Statement by the ICRC delivered by Tilman Rodenhauser, Legal Advisor, at the 7th substantive meeting of the Open-Ended Working Group on security of and in the use of information and communications technologies 2021-2025 New York 6 March 2024. "Focus on cyber operations that cause physical damage is not enough." Accessed May 20, 2024. https://www.icrc.org/en/oewg-cyber-new-statement.

United Nations Cyber Toolkit. "Interactive Toolkit." Accessed May 17, 2024. https://cyberlaw.ccdcoe.org/wiki/Main_Page.

4. Reports, guidelines, and other sources: national level

§1. Australia

Commonwealth of Australia, Department of Foreign Affairs and Trade. *Australia's International Cyber Engagement Strategy* (4 October 2017).

Commonwealth of Australia, Australian institute on international affairs. "Data as military objective (20 September 2018)." Accessed June 6, 2024. https://www.internationalaffairs.org.au/australianoutlook/data-as-a-military-objective/.

Commonwealth of Australia, Department of Foreign Affairs and Trade. *Comments on the draft of the report of the United Nations Open-ended Working Group* (16 April 2020).

Commonwealth of Australia, Department of Foreign Affairs and Trade. *Annex B to the 2020 International Cyber and Technology Engagement Strategy: position on how international law applies to State conduct in cyberspace* (5 November 2020).

Commonwealth of Australia, Department of Foreign Affairs and Trade. *Australia's submission to the report of the United National Group of Governmental Experts on Cyber* (28 May 2021).

Commonwealth of Australia, Department of Foreign Affairs and Trade. *Australian Cyber Security Strategy 2023-2030* (1 January 2023).

Commonwealth of Australia, Department of Foreign Affairs and Trade. *Cyber threat report 2022-2023* (14 November 2023).

§2. Belgium

Belgian Intelligence Studies Center. *Cyber Security* (19 November 2012).

Centre for Cyber Security Belgium. *Cyber Security Strategy 2021-2025* (1 May 2021).

Belgian Federal Public Service Foreign Affairs. *Communication* (18 January 2022).

§3. Brazil

Brazil. Comments on the draft of the report of the United Nations Open-ended Working Group (8 April 2020).

Brazil. Official Statement to the United Nations Group of Governmental Experts on Cyber (10 May 2021).

Brazil. "National Position: contribution to the United Nations Group of Governmental Experts on Cyber (August 2021)." Accessed June 6, 2024. https://cyberlaw.ccdcoe.org/wiki/National_position_of_Brazil_(2021).

Brazil. Official Statement after cyberattack against Brazilian Ministry of Health (10 December 2021).

Brazil. Cyber Security Strategy (8 August 2023).

§4. Chile

Chile. "Cyber Security Strategy 2017-2022 (1January 2017)." Accessed May 1, 2024. https://www.itu.int/en/ITUD/Cybersecurity/Documents/National_Strategies_Repository/Chile_NCSP%20%28ENG%29.pdf.

Chile. "State Report: international law applicable to cyberspace (21 October 2022)." Accessed May 1, 2024. https://www.oas.org/en/sla/iajc/docs/CJI-doc_671-22_rev2_corr1_ENG.pdf.

Chile. *Official Statement after cyberattack against the government of Chile* (17 October 2023).

§5. Denmark

Denmark. *National Position: contribution to the United Nations Group of Governmental Experts on Cyber* (July 2013).

Denmark. *Military Manual on international law relevant to Danish armed forces in international operations* (September 2016).

Danish Government. *Danish Cyber and Information Security Strategy* (May 2018).

Denmark. *Military Manual* (January 2020).

Danish Ministry of Defence. *Official Statement* (3 November 2022).

Denmark. *Official Statement after cyberattack on companies in the energy industry* (8 December 2023).

§6. Finland

Finnish Centre for Strategic and International Studies. *Cyber Security Strategy* (8 May 2011).

Finland. “Nordic Statement at the Open-ended Working Group on developments of information and telecommunications in the context of international security (10 February 2020).” Accessed June 6, 2024. https://finlandabroad.fi/web/un/nordic-statements/-/asset_publisher/7AjSWaX3YnO3/content/nordic-statement-open-ended-working-group-on-developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-second-substantive-session/384951.

Finland. “National Position: contribution to the United Nations Group of Governmental Experts (October 2020).” Accessed June 6, 2024. https://cyberlaw.ccdcoe.org/wiki/National_position_of_Finland_(2020).

Finland. *National Position on public international law in cyberspace* (15 October 2020).

Finnish Ministry of Foreign Affairs. *Official Statement* (October 2020).

Finnish Government. *Defence Report* (September 2021).

Finland. *Official Statement to the United Nations Open-ended Working Group on ICTs in the context of international security* (April 2022).

Finland. *Official Statement after cyberattack on the website of the Finnish government* (8 April 2022).

§7. France

French Ministry of Defence. *White Paper on Defence and National Security* (9 July 2008).

France. *Cyberdefence Policy* (8 June 2012).

France. *Cyber Security Report* (March 2017).

French Ministry of Defence. *Report International Law applicable to operations in cyberspace* (12 November 2018).

France. *Official Statement to the United Nations Open-ended Working Group on international law applied to operations in cyberspace* (14 July 2021).

§8. Germany

German Federal Ministry of Defence. *Manual on the law of armed conflict* (1 May 2013).

Germany. *Official Statement after Bundestag Hack* (1 May 2015).

Germany. *Official Statement after cyber-attack against German government’s network* (18 March 2018).

Germany. “National Position: contribution to the United Nations Group of Governmental Experts (6 April 2020).” Accessed June 6, 2024. https://www.justsecurity.org/75242/germanys-positions-on-international-law-in-cyberspace/.

Germany. *National Position on public international law in cyberspace* (1 March 2021).

German Ministry of Defence. *Position Paper: Cyber Operations* (16 March 2021).

§9. Israel

Israel. National Cybernatic Taskforce (18 May 2011).

Israel. Comments on the draft of the report of the United Nations Open-ended Working Group (1 April 2020).

Israel. Official Statement after cyberattack on Israel’s water facilities (25 April 2020).

Israel. Perspective on key legal and practical issues concerning application of international law to cyber operations (9 December 2020).

Israel. “Israel’s Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations (26 January 2021).” Accessed May 1, 2024. https://digital-commons.usnwc.edu/ils/vol97/iss1/21.

Israel. Official Statement on the application of international law to cyberspace (25 October 2021).

§10. New Zealand

New Zealand. Manual on the Law of Armed Conflict (7 August 2017).

New Zealand. *National Position: contribution to the United Nations Group of Governmental Experts* (February 2020).

New Zealand. Official Statement on the application of international law to cyberspace (1 December 2020).

§11. Norway

Ministry of Defence. *Manual on the law of armed conflict* (19 March 2013).

Norway. *Oslo Manual on Select Topics of the Law of Armed Conflict* (9 October 2020).

Norway. *National Position: contribution to the United Nations Group of Governmental Experts* (13 July 2021).

Norway. *Official Statement on the application of international law to cyberspace* (4 July 2023).

§12. Romania

Romanian Ministry of National Defence. *The Military Strategy of Romania* (1 January 2016).

Romania. *Official Statement: the security fears that keep European awake at night* (1 July 2018).

Romania. "Voluntary national contribution on the subject of how international law applies to the use of information and communications technologies submitted in the Group of Governmental Experts (13 July 2021)." Accessed June 6, 2024. https://cyberlaw.ccdcoe.org/wiki/National_position_of_Romania_(2021).

§13. Switzerland

Switzerland. *Report on the Security Policy* (23 June 2010).

Switzerland. *Law Manual of Air and Missile Warfare* (1 March 2017).

Switzerland. *National Position: contribution to the United Nations Group of Governmental Experts* (9 April 2020).

Switzerland. "National Position: public international law in cyberspace (18 March 2021)." Accessed June 6, 2024. https://docs-library.unoda.org/Open Ended_Working_Group_on_Information_and_Communication_Technologies_(2021)/20230308_Switzerland_submission_OEWG_international_law_as_delivered.pdf.

Switzerland. *Official Statement: maintaining international peace and security in cyberspace* (29 June 2021).

Switzerland. *Official Statement* (10 March 2023).

Switzerland. *Official Statement after cyberattacks* (2 November 2023).

§14. United States

United States. *Cyberspace Review Policy* (1 May 2011).

United States. *US Department of State* (18 December 2012).

United States. *Official Report on the Tallinn Manual and US Cyber Policy* (18 February 2013).

United States. *National Position: public international law in cyberspace* (1 April 2016).

United States. *Cyberspace Operations Report* (8 June 2018).

United States. *Legal Conference: Cyber Warfare and the Law of Armed Conflict* (18 April 2023).

CASE LAW & CASE LAW RELATED

1. International level

The case of the SS 'Lotus' (France v Turkey), Permanent Court of International Justice (PCIJ), 7 September 1927 (Lotus Case).

Anglo-Norwegian Fisheries Case (United Kingdom v Noway), ICJ Reports 1951, International Court of Justice (ICJ), 18 December 1951 (Fisheries Case).

North Sea Continental Shelf Cases (Federal Republic of Germany v Denmark and Federal Republic of Germany v Netherlands), ICJ Reports 1969, 3, International Court of Justice (ICJ), 20 February 1969 (North Sea Continental Shelf Cases).

Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v United States of America), ICJ Reports 1986, 14, International Court of Justice (ICJ), 27 June 1986 (Nicaragua case).

Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, ICJ Reports 1996, 226, International Court of Justice (ICJ), 8 July 1996 (Nuclear Weapons Case).

The Prosecutor v Duško Tadić, International Criminal Tribunal for the former Yugoslavia (ICTY), 15 July 1999 (Tadić Case).

Accordance with international law of the unilateral declaration of independence in respect of Kosovo (Declaration of Judge Simma), ICJ Reports Advisory Opinions 2010, International Court of Justice (ICJ), 22 July 2010 (Kosovo Case).

Jurisdictional Immunities of the State (Germany v Italy: Greece intervening), ICJ Reports 2012, 99, International Court of Justice (ICJ), 3 February 2012 (Jurisdictional Immunities Case).

Obligations concerning Negotiations relating to Cessation of the Nuclear Arms Race and to Nuclear Disarmament (Marshall Islands v United Kingdom), ICJ Reports 2016, International Court of Justice (ICJ), 5 October 2016 (Marshall Islands Case).

2. National level

§1. Australia

Australian Securities and Investments Commission v RI Advice Group Pty Ltd, Federal Court of Australia, 5 May 2022.

CR-19-02064, Criminal Division of County Court of Victoria, Melbourne, 20 November 2020.

§2. Belgium

AR P.04.0974.F, Court of Cassation, Second Chamber, 10 November 2004.

AR P.10.1094.F, Court of Cassation, 5 January 2011.

AR P.16.0048.N/1, Court of Cassation, 24 January 2017.

No. 2007/81, Criminal Court of Dendermonde, 14 May 2007.

Criminal Court of Hasselt, Fifteenth Chamber, 21 January 2004.

§3. France

N° 20/07493, Court of Appeal of Lyon, Eigth Chamber, 10 November 2021.

N° 19/00160, Court of Appeal of Versailles, Fifth Chamber, 3 December 2020.

§4. Germany

28 O 328/21, Regional Court of Köln, 18 May 2022.

§5. New Zealand

CIV-2021-485-379, High Court of New Zealand, 4 August 2021.

CIV-2020-404-000609, High Court of New Zealand, 2 March 2023.

§6. United States

McMorris, United States Federal Court of Appeals for the Second Circuit, 1 April 2021.

Stockx Customer Data Security Breach Litigation, United States Federal Court of Appeals for the Sixth Circuit, 2 December 2021.

SECONDARY SOURCES

1. Books

Adams, Maurice, and John Griffiths. "Against comparative method: explaining similarities and differences." In *Practice and theory in comparative law*, edited by Maurice Adams and Jacco Bomhoff, 279-301. Cambridge: Cambridge University Press, 2012.

Ammann, Odile. *Domestic Courts and the Interpretation of International Law: Methods and Reasoning Based on the Swiss Example.* Leiden: Brill Nijhoff, 2020. https://doi.org/10.1163/9789004409873.

Black-Branch, Jonathan L. *The treaty prohibitions on Nuclear Weapons: legal challenges for military doctrines and deterrence policies.* Cambridge: Cambridge University Press, 2021.

Bourgeois, Hanna, and Jan Wouters. "Methods of identification of international custom: a new role for opinio juris?" In *Global Justice, Human Rights and the Modernization of International Law*, edited by Riccardo Piscillo Mazzeschi and Pasquale de Sena, 69-111. Cham: Springer international Publishing, 2018.

Byers, Michael. *Custom, Power and the Power of Rules: International Relations and Customary International Law.* Cambridge: Cambridge University Press, 1999.

Choi, Stephen J., and Mitu Gulati. "Customary international law: how do courts do it?" In *Custom's Future: International Law in a Changing World*, edited by Curtis A. Bradley, 117-147. Cambridge: Cambridge University Press, 2016.

Crawford, Emily. *Non-binding Norms in International Humanitarian Law: Efficacy, Legitimacy and Legality.* Oxford: Oxford University Press, 2021.

D'Aspremont, Jean. "Non-State Actors and the formation of international customary law: unlearning some common tropes." In *Non-State Actors and the formation of customary international law*, edited by Ian Scobbie and Sufyan Droubi. Manchester: Manchester University Press, 2020.

Distefano, Giovanni, *Fundamentals of Public International Law: A Sketch of the International Legal Order.* Brill: Nijhoff, 2019. https://doi.org/10.1163/9789004396692.

Fuentes, Carlos Iván. *Normative Plurality in International Law: A Theory of the Determination of Applicable Rules.* Berlin: Springer, 2016.

Green, James A. *The persistent objector rule in international law.* Oxford: Oxford University Press, 2016.

Hakimi, Monica. "Custom's method and process in custom's future." In *Custom's Future: International Law in a Changing World*, edited by Curtis A. Bradley, 148-171. Cambridge: Cambridge University Press, 2016.

Haljan, David. *Separating powers: international law before national courts.* Den Haag: Asser Press, 2013.

Henckaerts, Jean-Marie, and Louise Doswald-Beck. *ICRC: Customary International Humanitarian Law: Volume I: Rules.* Cambridge: Cambridge University Press, 2009.

Hernández, Gleider. *International Law*. Oxford: Oxford University Press, 2019.

Hutchinson, Terry C. M., *Researching and Writing in Law: Third Edition*. Pyrmont: N.S.W.: Thomson Reuters/Lawbook Co., 2010.

Kestemont, Lina, *Handbook on Legal Methodology: From Objective to Method*. Antwerp: Intersentia, 2018.

Klabbers, Johannes Antonius Maria, and August Reinisch. "Sources of international organizations law: reflextions on accountability." In *The Oxford Handbook on the Sources of International Law*, edited by Jean d'Aspremont and Samantha Besson, 987-1006. Oxford: Oxford University Press, 2017.

Kolb, Robert. *Advanced Introduction to International Humanitarian Law.* Cheltenham: Edward Elgar Publishing, 2014.

Kontou, Nancy. *The Termination and Revision of Treaties in the Light of New Customary International Law*, *Oxford Monographs in International Law.* Oxford: Clarendon, 1994.

La Haye, Eva. *War crimes in internal armed conflicts*. Cambridge: Cambridge University Press, 2008.

Lepard, Brian D. *Customary International Law: A New Theory with Practical Applications.* Cambridge: Cambridge University Press, 2010.

Lepard, Brian. "Reexamining Customary International Law." In *Custom's Future: International Law in a Changing World*, edited by Curtis A. Bradley. Cambridge: Cambridge University Press, 2016.

Lusa Bordin, Fernando, Andreas Th. Müller, and Francisco Pascual-Vives. *The European Union and Customary International Law.* Cambridge: Cambridge University Press, 2022.

Maxwell, Jospeh A. *Qualitative Research Design. An Interactive Approach.* New York: Sage, 2013.

Müller, Andreas Th. "The direct effect of Customary International Law: The Treaty Analogy' and Its Limits." In *The EU and customary international law*, edited by Fernando Lusa Bordin, Andreas Th. Müller and Francisco Pascual-Vives, 210-239. Cambridge: Cambridge University Press, 2022.

Palchetti, Paolo. "The Role of General Principles in Promoting the Development of Customary International Rules." In General Principles and the Coherence of International Law, edited by Paolo Palchetti, 47-59. Leiden: Brill Nijhoff, 2019. https://doi.org/10.1163/9789004390935_005.

Ratner, Steven R. "Sources of International Humanitarian Law and International Criminal Law: War/Crimes and the Limits of the Doctrine of Sources." In *The Oxford Handbook of the Sources of International Law*, edited by Jean d'Aspremont and Samantha Besson, 912-936. Oxford: Oxford University Press, 2018.

Saunders, Imogen. *General Principles as a Source of International Law: Art. 38(1)(C) of the Statute of the International Court of Justice*. London: Bloomsbury Publishing, 2021.

Schmitt, Michael N., ed. *Tallinn Manual 2.0 on the International Law applicable to cyber-operations prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence*. Cambridge: Cambridge University Press, 2017.

Thirlway, Hugh. *The sources of International law: Second Edition.* Oxford: Oxford University Press, 2019.

Trachtman, Joel P. "The growing obsolescence of customary international law." In *Custom's Future: International Law in a changing world*, edited by Curtis A. Bradley, 172-204. Cambridge: Cambridge University Press, 2016.

Van Steenberghe, Raphaël. "Sources of International Humanitarian Law and International Criminal Law: Specific Features." In *The Oxford Handbook of the Sources of International Law*, edited by Jean d'Aspremont and Samanta Besson, 891-911. Oxford: Oxford University Press, 2018.

Verschuren, Piet, and Hans Doorewaard. *Designing a Research Project*. The Hague: Eleven Publishing, 2010.

Villiger, Mark Eugen. *Customary International Law and Treaties: A Manual on the Theory and Practice of the Interrelation of Sources.* Leiden: Martinus Nijhoff Publishers, 1997.

2. Journal articles

Azaria, Danae. "Codification by interpretation: The International Law Commission as an interpreter of international law." *The European journal of international law*, no. 31 (2020): 171-200.

Baker,Roozbeh (Rudy) B. "Customary international law in the 21st Century: Old Challenges and New Debates." *European Journal of International Law* 21, no. 1 (1 February 2010): 173–204. https://doi.org/10.1093/ejil/chq015.

Blutman, László. "Conceptual Confusion and Methodological Deficiencies: Some Ways That Theories on Customary International Law Fail." *European Journal of International Law* 25, no. 2 (1 May 2014): 529-552. https://doi.org/10.1093/ejil/chu034.

Crootof, Rebecca. "Change without Consent: How Customary International Law Modifies Treaties." *Yale Journal of International Law* 41, no. 2 (2016): 237-300.

Dordeska, Marija. "The process of International Law-making: The relationship between the International Court of Justice and the International Law Commission." *ICLR* 15, no. 1 (2015): 7-57.

Droege, Cordula. “Get off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians.” *International Review of the Red Cross* 94, no. 886 (June 2012): 533–578. https://doi.org/10.1017/S1816383113000246.

Eggett, Craig. “The Role of Principles and General Principles in the “Constitutional Processes” of International Law.” *Netherlands International Law Review* 66, no. 2 (July 2019): 197-217. https://doi.org/10.1007/s40802-019-00139-1.

Geiß, Robin, and Henning Lahmann. “Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space.” *Israel Law Review* 45, no. 3 (November 2012): 381–399. https://doi.org/10.1017/S0021223712000179.

Gisel, Laurent, 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.” *International Review of the Red Cross* 102, no. 913 (April 2020): 287–334. https://doi.org/10.1017/S1816383120000387.

Grote, Tatjana. “Best of Both Worlds? The Interplay between International Human Rights Law and the Law of Armed Conflict in Cyberspace.” *LSE Law Review*, no. 8 (2023): 179-226.

Gül, Yunus Emre. “Changing Notion of Object and Targeting Data Under the Law of Armed Conflict.” *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi* 27, no. 2 (December 2021): 1298–1313.

Hakimi, Monica. “Making sense of customary international law.” *Michigan Law Review* 118, (2020): 1487-1538.

Harrison Dinniss, Heather A. “The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives.” *Israel Law Review* 48, no. 1 (March 2015): 39–54.

Heller, Kevin Jon. “Specifically-affected States and the formation of custom.” *The American Society of International Law*, no. 1 (2018).

Jarose, Joanna. “Reconsidering the Definition of “attack” and “Damage” in Cyber Operations during Armed Conflict: Emerging Subsequent State Practice.” *TheAdelaide Law Review* 1, (December 2023): 317-338. https://search.informit.org/doi/abs/10.3316/informit.514594046455151.

Kent, Avidan, and Jamie Trinidad. “International Law Scholars as *Amici Curiae* : An Emerging Dialogue (of the Deaf)?” *Leiden Journal of International Law* 29, no. 4 (December 2016): 1081-1101. https://doi.org/10.1017/S0922156516000510.

Lahmann, Henning. “State Behaviour in Cyberspace: Normative Development and Points of Contention.” *Zeitschrift Für Außen- Und Sicherheitspolitik* 16, no. 1 (March 2023): 31–41.

Lekkas, Sotirios-Ioannis, and Panos Merkouris. “Interpretation of International Law: Rules, Content, and Evolution.” *Netherlands International Law Review* 69, no. 2 (September 2022): 183-189. https://doi.org/10.1007/s40802-022-00226-w.

Mačák, Kubo. “Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law.” *Israel law Review*, no. 48 (2015): 55-80.

Mačák, Kubo. “From the Vanishing Point Back to the Core: The Impact of the Development of the Cyber Law of War on General International Law.” *9th International Conference on Cyber Conflict (CyCon)* (2017): 1–14.

McKenzie, Simon. “Cyber Operations against Civilian Data: Revisiting War Crimes against Protected Objects and Property in the Rome Statute.” *Journal of International Criminal Justice* 19, no. 5 (1 November 2021): 1165–1192. https://doi.org/10.1093/jicj/mqab067.

Pascucci, Peter. “Distinction and Proportionality in Cyber War: Virtual Problems with a Real Solution.” *Minnesota Journal of International Law*, no. 26 (2017): 419-460.

Petersen, Niels. “The International Court of Justice and the Judicial Politics of Identifying Customary International Law.” *European Journal of International Law* 28, no. 2 (May 2017): 357-385. https://doi.org/10.1093/ejil/chx024.

Sari, Aurel. “Hybrid Threats and the Law: Concepts, Trends and Implications.” *Hybrid CoE Trend Report*, no. 3 (April 2020): 1-28.

Sender, Omri, and Michael Wood. “A Mystery No Longer? Opinio Juris and Other Theoretical Controversies Associated with Customary International Law.” *Israel Law Review* 50, no. 3 (November 2017): 299-330. https://doi.org/10.1017/S0021223717000115.

Schmitt, Michael N., and Sean Watts. “The Decline of International Humanitarian Law Opinio Juris and the Law of Cyber Warfare.” *Texas International Law Journal* 50, no. 2–3 (2016): 189–232.

Schmitt, Michael N. “Wired Warfare 3.0: Protecting the Civilian Population during Cyber Operations.” *International Review of the Red Cross* 101, no. 910 (April 2019): 333–355. https://doi.org/10.1017/S1816383119000018

Scoville, Ryan M. “Finding Customary International Law.” *Iowa Law Review* 101, (2016): 1894-1948.

Sohail, Humna. “Fault Lines in the Application of International Humanitarian law to Cyberwarfare.” *The Journal of Digital Forensics, Security and Law : JDFSL* 17 (2022): 1–13.

Son, Hye-Ryon, Son-Gyong Jong, Won-U Kang, Myong-Il Ri, Yun-Chol Ko, and Hui-Chol Pak. “Reassessment of the “General Principles of Law” Referred to in Article 38(1)(c) of the ICJ Statute.” *International Studies (New Delhi)* 59, no. 2 (2022): 144-162. https://doi.org/10.1177/00208817221100912.

Talbot Jensen, Eric. “The Tallinn Manual 2.0: highlights and insights.” *Georgetown Journal of International Law,* no. 48 (2017): 735.

Talmon, Stefan. “Determining Customary International Law: The ICJ’s Methodology between Induction, Deduction and Assertion.” *European Journal of International Law* 26, no. 2 (May 2015): 417–443. https://doi.org/10.1093/ejil/chv020.

Wood, Michael. “The present position within the ILC on the topic “Identification of customary international law”: in partial response to Sienho Yee, Report on the ILC Project on

"Identification of Customary International Law." *Chinese Journal of International Law,* (2016): 3-15.

Zammit Borda, Aldo. "A Formal Approach to Article 38(1)(d) of the ICJ Statute from the Perspective of the International Criminal Courts and Tribunals." *European Journal of International Law* 24, no. 2 (2013): 649-661. https://doi.org/10.1093/ejil/cht023.

3. Website content

Dark Reading. "New research suggests Africa is being used as a 'testing ground' for nation state cyber warfare." Accessed May 1, 2024. https://www.darkreading.com/cybersecurity-operations/new-research-suggests-africa-is-being-used-as-a-testing-ground-for-nation-state-cyber-warfare.

DeepL. "DeepL Translate." Accessed May 19, 2024. https://www.deepl.com/translator.

EJIL Talk: Blog of the European Journal of International Law. "Israel's cautious perspective on International Law in cyberspace: part II (jus ad bellum and jus in bello)." Accessed April 15, 2024. https://www.ejiltalk.org/israels-cautious-perspective-on-international-law-in-cyberspace-part-ii-jus-ad-bellum-and-jus-in-bello/.

ICRC. "Who we are." Accessed May 20, 2024. https://www.icrc.org/en/who-we-are.

Kleinlein, Thomas. "Customary International Law and General Principles: Rethinking Their Relationship." SSRN Scholarly Paper. Accessed March 22, 2024. https://doi.org/10.2139/ssrn.2923964.

Mačák, Kubo. "Unblurring the Lines: Military Cyber Operations and International Law." Accessed April 23, 2023. https://www.tandfonline.com/doi/epdf/10.1080/23738871.2021.2014919?needAccess=true&role=button.

Marxsen, Christian. "What Do Different Theories of Customary International Law Have to Say About the Individual Right to Reparation Under International Humanitarian Law?" Accessed May 17, 2024. https://www.zaoerv.de.

Sender, Omri, and Michael Wood. "The International Court of Justice and Customary International Law: a reply to Stefan Talmon." Accessed March 22, 2024. https://www.ejiltalk.org/the-international-court-of-justice-and-customary-international-law-a-reply-to-stefan-talmon/.

Schmitt, Michael M. N. "The Notion of 'Objects' During Cyber Operations: A Riposte in Defence of Interpretive and Applicative Precision." SSRN Scholarly Paper. Accessed May 20, 2024. https://papers.ssrn.com/abstract=2557989.

Stephan, Paul B. "Big Data and the Future Law of Armed Conflict in Cyberspace." Accessed March 20, 2024. https://papers.ssrn.com/abstract=3521387.

Talmon, Stefan. “Determining Customary International Law: the ICJ’s Methodology and the Idyllic World of the ILC.” EJIL Talk. Accessed May 17, 2024. https://www.ejiltalk.org/determining-customary-international-law-the-icjs-methodology-and-the-idyllic-world-of-the-ilc/.

The Wire. “State-sponsored cyberattacks against India went up by 278% between 2021 and September 2023: Report.” Accessed May 1, 2024. https://thewire.in/tech/state-sponsored-cyber-attacks-against-india-went-up-by-278-between-2021-and-september-2023report#:~:text=New%20Delhi%3A%20State%2Dsponsored%20cyber,a%20new%20report%20has%20found.

US Army. “US Army Investing Additional 25 million in Cybersecurity.” Accessed December 19, 2023. https://www.thedefensepost.com/2021/07/13/us-army-cybersecurity/.

Clapson, Colin. “Belgium invests extra 14 billion euros in defence over the next eight years.” VRT News. Accessed December 19, 2023. https://www.vrt.be/vrtnws/en/2022/01/27/belgium-to-announce-major-defence-investments/.

Wong, Jing Zhi. “Comparative Legal Methodology and Its Relation to the Identification of Customary International Law.” SSRN Scholarly Paper. Accessed March 22, 2024. https://papers.ssrn.com/abstract=3655195.

ANNEX 1: SCENARIOS

This annex contains examples of the most often reoccurring types of cyber operations. They are used to show the various effects a cyber operation against data can have. The first scenario of each cyberattack is a fictional situation, written by GEISS and LAHMANN.[331] Most of these hypothetical situations occur in an armed conflict. The second scenario of each type of operation consist of real-life events that have remained vague from a legal perspective: were these attacks lawful or not? The main reason for this is because no cyber armed conflict has been to date qualified as such to date.

CYBER OPERATION 1: RANSOMWARE ATTACK

Scenario A: Ransomware operation against a hospital.

"*During a situation of armed conflict, the military of State A carries out a ransomware operation against the servers of a major hospital in State B that store the patients' case files, encrypting them until State A is willing to withdraw its troops from a contested island located on the continental shelf of State B. No patient suffers physical harm, but a great number of surgeries and other essential medical treatments must be postponed, and a couple of persons need to be transferred to other hospitals. In a variation of this scenario, the operation is only seemingly a ransomware attack. In fact, the military of State A employs a wiper malware, which immediately leads to the destruction of all patient files on the affected server, requiring hospital staff to recreate the files on paper from scratch.*"[332]

Scenario B: Springhill Medical Center ransomware attack (2019)

In July 2019, the Springhill Medical Center, a hospital in Mobile Alabama in the United States of America came under attack by allegedly the Wizard Spider. This is a Russian cybercrime group which had already targeted not only hospitals, but also businesses and government institutions. Wizard Spider encrypted files and attacked the Microsoft Windows-based systems to oblige the hospital to pay a ransom. When the Medical Center realised it was under attack, it

[331] Geiß and Lahmann, "Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space," 381–99.
[332] *Ibidem.*

immediately had to shut down its system because it refused to pay the ransom. Access to certain medical equipment and health records was therefore impossible.[333]

In addition, the usual number of medical staff at the labour and delivery unit checking the monitors had significantly shrunk, since it had to resort to phone communication with the other services. Because of this lack of staff, no one noticed that the umbilical cord was wrapped around a child's neck during the delivery. The child died nine months later due to severe brain damage. The mother has filed a negligence suit against the hospital. If the causality between the attack and the child's death is proven, the child will be considered the first casualty of a cyber operation.[334]

CYBER OPERATION 2: FINANCIAL DAMAGE

Scenarion A: Financial damage through data leaks

"A few days before the company's initial public offering (IPO) at the national stock exchange, the military of State B launches a cyber operation against the IT systems of Company C, which is headquartered in State A. The two States have been engaged in an armed conflict for the past year. The military cyber unit extracts a large file containing sensitive business data which expose a financial scandal involving the leadership of Company C, the CEO of the national stock exchange, and the heads of the national financial supervision authority. State B subsequently leaks the data through a non-governmental organisation which specialises in exposing classified information and other secrets. As a result, the IPO of Company C is cancelled and the stock market crashes, which leads to considerable economic damage and to a sustained rise in unemployment in State A."[335]

Scenario B: The Colonial Pipeline attack (2021)

In 2021, the Colonial Pipeline Company, one of the biggest fuel suppliers in the USA, was the victim of a cyberattack. Through stealing nearly 100 GB of data, the attack resulted in a

[333] "Cyber Toolkit: Springhill Medical Center ransomware attack (2019)", UN, accessed November 2, 2023, https://cyberlaw.ccdcoe.org/wiki/Springhill_Medical_Center_ransomware_attack_(2019).
[334] *Ibidem.*
[335] Geiß and Lahmann, "Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space," 381–99.

disruption of the company's accountancy and the preventive closure of the distributive network. Because of a panic reaction, there was a buyout of fuel. Consequently, there was a fuel shortage, making the prices much higher than before. The US government pointed towards a Russian hacking group for having *"some responsibility"* in the act. Russia never took up that responsibility whatsoever.[336]

CYBER OPERATION 3: ESSENTIAL FACILITIES (ELECTRICITY, WATER, …)

Scenario A: Cyber operation against water treatment facility

"*During a situation of armed conflict, the military of State A engages in an offensive cyber operation against the industrial control systems (ICS) of a water treatment facility in State B, altering critical datasets essential for the maintenance of the correct level and mixture of chemicals for processing the drinking water for a major city. As employees notice the tampering, they carry out an emergency shutdown of the facility, which leads to minor water shortages in the city for three days.*"[337]

Scenario B: Notpetya (2017)

On the night of 27 to 28 June 2017, the Russian Federation (allegedly) cast a cyberattack on the Ukrainian public and private sector. NotPetya malware was spread across a well-known software, mostly used by businesses and the government, which encrypted their data. This led to an estimated global loss of more than 10 billion (American) dollar. Moreover, the radiation monitoring system at Ukraine's Chernobyl Nuclear Power Plant was shut down for a significant amount of time.[338]

CYBER OPERATION 4: DATA LEAKAGE

Scenario A: Data collection and release 3.0

---

[336] "Cyber Toolkit: Interactive Toolkit," UN, accessed May 17, 2024, https://cyberlaw.ccdcoe.org/wiki/Main_Page.

[337] Geiß and Lahmann, "Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space," 381–99.

[338] "Cyber Toolkit: NotPetya (2017)", UN, accessed November 2, 2023. https://cyberlaw.ccdcoe.org/wiki/NotPetya_(2017).

"Exploiting a vulnerability in one of the servers of Company C, the major State-owned petroleum and natural gas company in State A, a religious and socially conservative country is in a protracted situation of armed conflict with State B, the latter's military cyber unit deploys the Mimikatz tool in order to obtain the passwords of the company's employees. Using the stolen password of one of the executives, the military hackers manage to extract terabytes of unencrypted emails and the social security numbers from employees which contain both business and private information. Among other things, a number of emails reveal intimate facts such as the homosexuality of a couple of employees, which is a felony punishable by imprisonment in State A. Pretending to be citizens of State A which belong to an organisation concerned with 'religious purity', service members of the cyber unit leak the sensitive information to major newspapers in State A who subsequently publish stories about the respective employees, leading to criminal indictments and death threats. State B's military furthermore sells the obtained social security numbers on the dark web."[339]

Scenario B: Sony Pictures Entertainment Attack (2014)

On 24 November 2014, Sony realised that a group of hackers had gained access to their internal network and database for over several months. The reason for this was (allegedly) the neglect of the request by the North Korean government to halt the release of a movie about the CIA and Kim Jong-un. Not only personal information (medical records, correspondence, social security numbers, …) of the Sony employees had been stolen, but also unreleased scripts which were later leaked all over the internet.[340]

CYBER OPERATION 5: DATA THEFT

Scenario A: digital blackmail

"*After a year of armed hostilities between States A and B, the military of State B hacks the IT systems of the largest cellphone and internet provider of State A. The hackers extract a large trove of data, among them the location data and call records of all customers. They also use*

[339] Geiß and Lahmann, "Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space," 381–99.

[340] "Cyber Toolkit: Sony Pictures Entertainment Attack (2014)", UN, accessed November 2, 2023. https://cyberlaw.ccdcoe.org/wiki/Sony_Pictures_Entertainment_attack_(2014).

the company's networks to secretly install surveillance software in one of the country's main internet exchange points, allowing State B to subsequently monitor the data traffic in State A in real time. The analysis of the phone and internet metadata reveals inter alia that member of parliament M, who belongs to the ruling party in State A, has been having an extramarital affair. The military of State B uses that information to coerce M into voting against a parliamentary act which would have significantly increased troop presence on the border between the two countries."[341]

Scenario B: Office of Personnel Management data breach (2015)

In 2013, an unknown group of hackers, (allegedly) sponsored by the Chinese government, broke into the servers of the United States Office of Personal Management. The attack remained unnoticed until April 2015. The sensitive information (address, birth date, social security number, …) of approximately 21.5 million individuals had been stolen, including 5.6 million fingerprints. A significant amount of employees have later on also stated that they have been subject to identity theft activities, such as fraudulent credit charges and tax filings.[342]

[341] Geiß and Lahmann, "Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space," 381–99.

[342] "Cyber Toolkit: Office of Personnel Management data breach (2015)", UN, accessed November 2, 2023. https://cyberlaw.ccdcoe.org/wiki/Office_of_Personnel_Management_data_breach_(2015).

ANNEX 2: SCHEME OF LITERATURE

This scheme provides an overview of the scholars who provided a statement about where State practice is heading, concerning the protection of data and the principle of distinction.[343] The scheme shows two inconsistencies. First, a majority of scholars in this debate state that State practice is heading towards considering data an object, consequently a civilian object for the principle of distinction. Although this is a majority, the scheme also shows that some authors do not believe this argument is true. Second, when authors give an example of State practice to back up their argument, their examples are inconsistent. These inconsistencies are underlined.

This shows that the quantity, as well as the quality of the evidence is insufficient to understand whether their statement is true. Hence, the master's thesis puts their statement into practice and verifies its truthfulness.

Author	**State practice evolving towards**	**Evidentiary State practice brought to support this claim**
Dinniss	Evolutive approach: 'some' data as a civilian object	/
Droege	Inconsistency	/
Geiss and Lahmann	Evolutive approach: 'some' data as a civilian object	/
Gisel *et al.*	Evolutive approach: 'some' data as a civilian object	/
Gul *et al.*	Evolutive approach: 'some' data as a civilian object	Austria, France, Germany
Macak	Evolutive approach: data as a civilian object	France, Germany

[343] Based on the Literature Review by Charlotte Teuwens, 2022-2023.

Mckenzie	Inconsistency	Austria (restrictive), Denmark (restrictive), France (evolutive), Israel (restrictive), Norway (evolutive). The Netherlands, The US, and the UK have given inconsistent opinions.
Schmitt	Restrictive approach	The US
Sohail	Restrictive approach	/

The UN Cyber Toolkit, scenario 12 summarises the two main approaches in the debate on the notions of data and object as well as their effect on the lawfulness of certain cyber operations in the following table. It must be mentioned that the UN itself emphasises that the law remains unsettled on this question. The table merely presents an overview, it does not take a stand in the debate.[344]

	Data ≠ object	**Data = object**
Incident 1 (cyber operations against military datasets)		Permissible insofar as the dataset fulfils both prongs of the definition of military objectives.
Incident 2 (cyber operations against essential civilian datasets)	Because data is not an 'object' for the purposes of IHL, it does not need to fulfil the criteria of a military objective for an operation against it to be lawful under IHL. Accordingly,	Prohibited due to the non-military character and use of the datasets in question.

[344] "Scenario 12: Cyber operations against computer data," UN Cyber Toolkit, accessed December 19, 2023, https://cyberlaw.ccdcoe.org/wiki/Scenario_12:_Cyber_operations_against_computer_data#:~:text=The%20ICRC%20has%20highlighted%20medical,essential%20component%20of%20digitalized%20societies%27.

	provided that other applicable rules of IHL are complied with, all of these cyber operations would be permissible under IHL.	
Incident 3 (cyber operations against non-essential civilian datasets)		Prohibited due to the non-military character and use of the datasets in question unless justified under the customary exception for psychological operations and propaganda.

ANNEX 3: RESEARCH STRATEGY

GENERAL COMMENTS

As mentioned in the text, the doctrine of specially affected States is not used in this thesis. A State regarded as specifically affected would add a hierarchy to the States researched: the international legal doctrine accepts that the evidence of specifically affected States can be more important for certain issues, without giving them a right to veto.[345] More notably, if a State is treated as specifically affected, then it is required to explicitly object to the emerging rule: mere silence is considered acceptance of the rule as such, because they have significant interest in the subject matter.[346]

Not only is the use of cyber activities in conflicts increasing, but also the number of States taking interest in these operations. To stay true to the aim of the research, it is crucial that during the year in which this master's thesis takes place, the researcher keeps an eye out for new cases or reports. To facilitate this, the researcher has subscribed to various databases of domestic case law of relevant States and of several international organisations. In this way, one must merely check upon the mailbox to ensure that no crucial source is missing.

PRIMARY SOURCES AND STATES CONSIDERED

This section shows the, at first glance, most important sources of the relevant States used for the evaluative research.[347] As mentioned, these criteria will be evaluated separately, but since some can be used for the evaluation of both the criteria if they are looked at from a different focus, they are presented together here. This provides the following presentation:

---

[345] *Fisheries (United Kingdom v. Norway),* ICJ Reports 1951 (Norwegian Fisheries case); *Obligations Concerning Negotiations relating to Cessation of the Nuclear Arms Race and to Nuclear Disarmament (Marshall Islands v. United Kingdom)*, ICJ Reports 2016 (Marshall Islands case); Kevin Jon Heller, "Specifically-affected States and the formation of custom," *The American Society of International Law*, no. 1 (2018).
[346] Heller, "Specifically-affected States and the formation of custom".
[347] Piet Verschuren and Hans Doorewaard, *Designing a Research Project* (The Hague: Eleven Publishing, 2010).

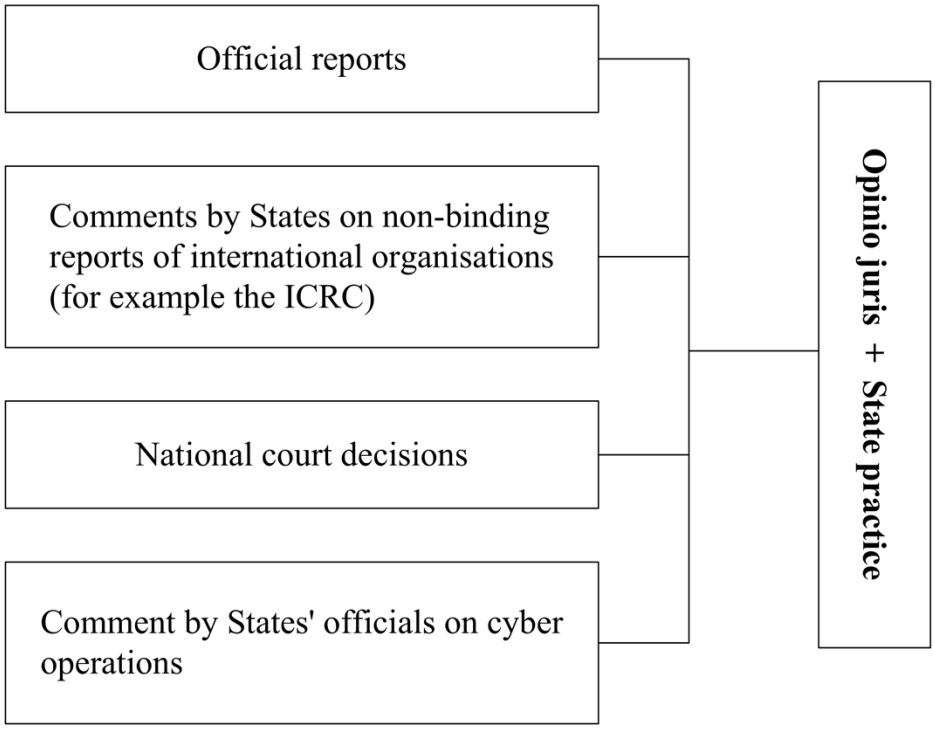

Figure 4: overview of the relevant sources

To find the most relevant sources, an abundance of methods is used. These include: the non-exhaustive list in the ILC draft conclusions and commentaries, data browsing, locating explanatory notes by State officials on the topic, looking at the relevant sources pointed out in the scholarly debate, the snowballing method, talking with supervisors, …

It is important to mention that not every type of source is present in the same amount in every relevant State. The most important one however, the official reports, must be published in every one of them, since this is one of the criteria on which the choice of States was made. This is treated as the most important source of information: it contains a lot of other relevant references, is a profound and well described document and can be used for both the evaluations.

When looking at these sources, special attention is paid to the language used. Does the State use definite terms, such as “shall”, “must” and “will”, or does it use hypothetical connotations, like “may”, “would” and “if”? The latter can be regarded a lack of support for the proposed emergence of custom.

There is no clear-cut answer to the question how much evidence is enough to conclude on the *opinio juris* of a State. It requires the assessment whether all relevant sources on the subject matter have been consulted. For the official State reports for example, this means that only the final published reports are used, not the draft versions, since these contain comments which were disregarded. A useful indicator is the following: once the info starts being repeated in several documents, there is no need for further research.[348]

[348] Terry C. M. Hutchinson, *Researching and Writing in Law* (Pyrmont: N.S.W.: Thomson Reuters/ Lawbook Co., 2010).

SEARCH FOR THE COURT DECISIONS

To find the relevant national court decisions, various terms were used similar to data protection. It contained of broad terms, synonyms, closely related terms, and related procedural terms used to browse the databases of the relevant courts. In general, the relevant court decisions were available in a for the author comprehensible language. The only few that required a translation, were translated using DeepL Translate.[349] This research can be summarised as follows:[94]

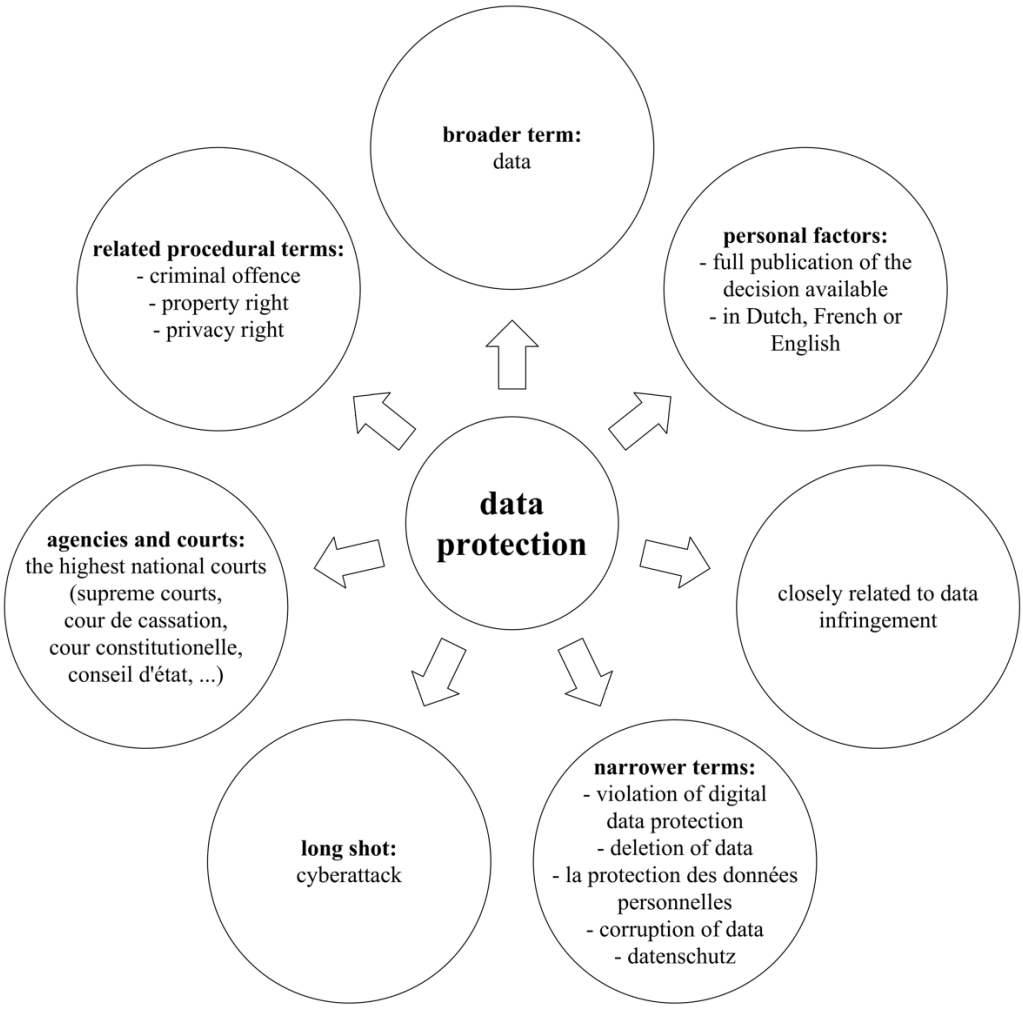

Figure 5: overview the terms used to find the relevant court decisions

[349] "DeepL Translate," DeepL, accessed May 19, 2024, https://www.deepl.com/translator.

ANNEX 4: OVERVIEW OF CONTACT WITH STATES

Country	Government	Cyber Defence Community	Answer Government	Answer Cyber Defence Community
Australia	Reminder 24/01 (Australian government: Australian signals directorate)	Reminder 24/01 (Australian cyber security cooperative research centre)	No reply	No reply
Belgium	Reminder 24/11	Reminder 24/11 (Centrum voor cybersecurity België)	No reply	No reply
Brazil	Reminder 24/01	Reminder 24/01 (Brazilian Research Network Computer Security Incident Response Team)	No reply	No reply
Chile	E-mailed 15/12 (Chilean atiende)	Not available for contact	Affirmative	Not available for contact
Denmark	E-mailed 15/12 (Agency for digital government)	E-mailed 15/12 (Centre for cyber security Denmark)	Affirmative	Unable to help
Finland	E-mailed 16/12 (Finnish ministry of defence and Finnish ministry of foreign affairs)	E-mailed 16/12 (National Cyber Security Centre of Finland)	Affirmative	Affirmative
France	E-mailed 21/11 (Sécrétariat général de la défense du gouvernement française de la sécurité nationale)	E-mailed 14/12 (Agence nationale de la sécurité des systèmes d'information)	Affirmative	Affirmative
Germany	E-mailed 17/12 (Federal ministry of the Interior Building	E-mailed 17/12 (National Coordination	Affirmative + addition blogpost	Affirmative

	and Community and Bundeskriminalamt)	Centre for Cybersecurity)		
Israel	Reminder 24/01 (The Federmann Cyber Security Research Center)	Not available for contact	No reply	No reply
New Zealand	E-mailed 17/12 (New Zealand justice government)	E-mailed 17/12 (National cyber Security Center New Zealand)	Affirmative + addition contact	Affirmative
Norway	E-mailed 18/12 (Norwegian ministry for defence)	E-mailed 18/12 (Norwegian Defence Research Establishment)	Affirmative	Affirmative
Romania	Reminder 24/01 (Romanian Ministry of national defence)	Reminder 24/01 (Romanian Cyber Security Defence Community)	No reply	No reply
Switzerland	Reminder 24/01 (UN Security Council Switzerland Delegation and Swiss federal Department of Defense,...)	Reminder 24/01 (Swiss Cyber Institute)	No reply	No reply
United States	Reminder 24/01 (US Department of Defense)	Reminder 24/01 (US Cybersecurity Community)	No reply	No reply

ANNEX 5: LIST OF EVALUATED STATES' ACTIVITIES

Annex 5 presents an overview of all the sources that were evaluated for this research on a potential emergence of a CIL rule on considering data an object under the principle of distinction. The analysis is specifically looking at State's views on whether a cyber operation that only targets data is governed by the IHL obligation to direct attacks only against military objectives and not against civilian objects. The sources are listed alphabetically and by ascending dates. There is no distinction made between a source useful for State practice or for *opinio juris*, since as earlier mentioned, these can use the same sources. The fourth column presents whether a State's national source presents itself affirmative or negative of the question whether data can be considered an object. In addition, the fifth and sixth column present (when possible) the reason given for this approach in the evidence, as well as additional remarks made on the topic which are accepted as useful.

State	Type of source	Date	Approach	Reason	Remarks
Australia	Australia's International Cyber Engagement Strategy	04/10/2017	Inconsistent	Principle of distinction applies and distinction must be made between civ and mil. But not explicit on 'data' as an object, unclear whether can *assume* that this follows from the fact that principle of distinction applies.	/
Australia	Australian institute on international affairs: data as military objective	20/09/2018	Affirmative	Reason: approach reflects the core humanitarian purpose of reducing the effects of conflict on the civilian population.	E.g. Data as military objective: digital weapons log. E.g. Civilian object: commercial database. Future questions: not "if", but how and when 'targetable' data is to be differentiated from non-targetable employment of data in espionage.
Australia	Comments on the draft of the report of the UN OEWG	16/04/2020	Inconsistent	Principle of distinction applies and distinction must be made between civ and mil. But not explicit on 'data' as an object, unclear whether can *assume* that this follows from the fact that principle of distinction applies.	/
Australia	Annex B to the 2020 International Cyber and Technology Engagement Strategy: position on how IL applies	05/11/2020	Inconsistent	Principle of distinction applies and distinction must be made between civ and mil.	/

	to State conduct in cyberspace			But not explicit on 'data' as an object, unclear whether can *assume* that this follows from the fact that principle of distinction applies.	
Australia	County Court of Victoria at Melbourne: Criminal Division: CR-19-02064	20/11/2020	Negative	Merely found guilty for cyberattacks targeting data that results in a physical disruption of a computer(system).	Not data as such, only data which results in a physical disruption.
Australia	Submission to the report of the UN GGE on Cyber	28/05/2021	Inconsistent	Principle of distinction applies and distinction must be made between civ and mil. But not explicit on 'data' as an object, unclear whether can *assume* that this follows from the fact that principle of distinction applies.	/
Australia	Criminal Code concerning computer offences: section 476 and following.	01/04/2022	Affirmative	478.1-478.4: unauthorised access, modification, impairment of data 478.5: new offence of "*dealing with data obtained by unauthorised access or modification*".	Sees the access, modification or impairment of data as of a physical element. 477.2-478.2: Aggravated offence if is directed against a critical infrastructure asset such as: telecom, broadcasting, domain name, banking/ insurance, financial market structure, water, electricity, gas, energy market operator, liquid fuel, hospital, education, food, port, freight

					infrastructure, public transport, aviation.
Australia	Federal Court of Australia: Australian Securities and Investments Commission v RI Advice Group Pty Ltd	05/05/2022	Affirmative	"*(...) targeting personal information*"; found responsible.	Risks are increasing, especially against personal sensitive information and one must provide sufficient cybersecurity.
Australia	Cyber security strategy 2023-2030	01/01/2023	Affirmative	Reason: "*Data that is safe today may not be tomorrow and failing to defend (...) will have detrimental consequences."*	/
Australia	Cyber threat report 2022-2023	14/11/2023	Affirmative	Reason: "*Protecting data, particularly sensitive personal information, is vital for the safety of the community (...).*"	Data of critical infrastructures mentioned: personal information, financial information, intellectual property and research, telecom.
Belgium	Criminal Court Hasselt, Fifteenth Chamber.	21/01/2004	Affirmative	Art. 550 Sw.: *"The mere theft or modification of data is sufficient. (...) The actual cyber infrastructure must not necessarily be damaged."*	/
Belgium	Court of Cassation, Second Chamber, *AR P.04.0974.F.*	10/11/2004	Negative	"*Damage caused to the data of computer programmes installed in a computer system is not damage caused to moving or powered devices and is not the offence referred to in art. 523 Sw.*"	/
Belgium	Criminal Court Dendermonde.	14/05/2007	Affirmative	Art. 550 Sw.: *"The mere theft or modification of*	/

				data is sufficient. (…) The actual cyber infrastructure must not necessarily be damaged."	
Belgium	Court of Cassation, *AR P.10.1094.F*	05/01/2011	Affirmative	"*The software, studies, reports, (…) documents, (…) present in an IT system may be assimilated to writings of any kind or other movable corporeal objects."*	/
Belgium	Belgian Intelligence Studies Center: Cyber Security	19/11/2012	Inconsistent	Principle of distinction applies and distinction must be made between civ and mil object. But not explicit on 'data' as an object, unclear whether can *assume* that this follows from the fact that principle of distinction applies.	In 2011, Belgium signed a memorandum for understanding with the Netherlands and Luxembourg for cooperation in cybersecurity to: share information and cooperate.
Belgium	Court of Cassation, *AR P.16.0048.N/1*	24/01/2017	Affirmative	Art. 550 Sw.: *"The mere theft or modification of data is sufficient. (…) The actual cyber infrastructure must not necessarily be damaged."*	/
Belgium	Cyber Security Strategy 2021-2025	01/05/2021	Affirmative	"*Is not only about disruption of infrastructure, but also about potential danger for integrity, availability, and confidentiality of data (…). The digitalisation of this information makes it hackable (…) and impacts*	Not only data resulting in a physical disruption, but also the mere destruction of data itself is of great concern. Points towards far reaching application.

				the general safety of citizens."	
Belgium	Communication FOD Buitenlandse zaken	18/01/2022	Inconsistent	In favour of first implementing and interpreting clearly already existing principles, like the principle of distinction, but not explicit about position of data in this principle: unclear whether can *assume* that this follows from the fact that principle of distinction applies.	/
Brazil	Comments on the draft report of the UN OEWG	08/04/2020	Inconsistent	Danger towards civilians because of interconnectedness. Affirms importance of IHL, strongly encourages inclusion of specific references to principles of IHL in relation to cybersecurity, like the principle of distinction. Does not, however, present its opinion on the interpretation itself	Specific reference of concern towards electrical, water and sanitation systems as critical infrastructures.
Brazil	Official Statement to the UN GGE	10/05/2021	Inconsistent	IHL applies in cyberspace, but concerns expressed about unqualified transfers of IHL and "*an unlimited right of self-defence could legitimise cyberspace as a military domain, while also challenging the protective value of sovereignty and cementing a*	Quite ambiguous opinion.

				Western-biased status quo."	
Brazil	National position: contribution to the UN GGE	01/08/2021	Inconsistent	"*IHL applies (…) and aim is to minimise human suffering (…) and provide a minimum level of protection to civilians (…). In making the assessment of (…) distinction, (…) parties must take into consideration the particularities of the cyberspace, such as the interconnectivity (…).*" But no explicit mention of data as an object: unclear whether can *assume* that this follows from the fact that principle of distinction applies.	Presumption in favour of a cyber infrastructure being dedicated to civilian purposes.
Brazil	Official statement after cyberattack against the Brazilian Ministry of Health	10/12/2021	Inconsistent	50TB worth of data containing the information of COVID-19 vaccinations of millions of citizens was copied and deleted. No comment on whether the deletion and theft of civilian data was considered theft of a civilian object.	/
Brazil	Brazil's cyber security strategy	08/08/2023	Inconsistent	IHL applies in cyberspace, but concerns expressed about unqualified transfers of IHL and "*an unlimited right of self-defence could legitimise cyberspace as a military domain, while also challenging the*	Believes there are two teams: team thinking of IHL applying to cyberspace, of which it is limited in favour, other team is China and Russia who want new rules, with whom it also maintains contacts.

				protective value of sovereignty and cementing a Western-biased status quo."	Is afraid of a too Western approach.
Chile	Chile's cyber security strategy 2017-2022	01/01/2017	Inconsistent	IHL applies in cyberspace and distinction must be made between civ and mil object. But not explicit on 'data' as an object, unclear whether can *assume* that this follows from the fact that principle of distinction applies.	"*To develop a strategy protecting private and public users*." "*The countries affected with the highest numbers of cyberattacks in Latin America were Brazil (…) Chile*."
Chile	State report: IL applicable to cyberspace	21/10/2022	Inconsistent	IHL applies in cyberspace; object must be visible and tangible, but nevertheless "*Chile recognises that an attack directed exclusively against computer data could generate adverse consequences affecting the civilian population, therefore, due to its effects, the principle of distinction must be taken into account and a State should refrain from attacking data in case it could affect the civilian population, unless such data were being used for military purposes*."	Link with the scale and effects approach in the context of the notion of 'attack' in rule 69 of TM 2.0: Chile seems to apply the same approach here in the debate around the notion of 'object'.
Chile	Official statement after cyberattack against government of Chile	17/10/2023	Inconsistent	Large attack on the National Customs Service, but no comment on whether this attack on data was considered an	/

				attack on a civilian object.	
Denmark	National position: contribution to the UN GGE	04/07/2013	Negative	IHL applies, the principle of distinction applies, but data cannot in and of itself be considered an object under IHL, there must be an adverse secondary effect on physical objects (= view in TM 2.0).	/
Denmark	Military Manual on international law relevant to Danish armed forces in international operations	01/09/2016	Inconsistent	IHL applies in cyberspace and distinction must be made between civ and mil object. But not explicit on 'data' as an object, unclear whether can *assume* that this follows from the fact that principle of distinction applies.	Cyberspace is regarded a military battle space, but Denmark does not provide further details on technical and operational aspects.
Denmark	Danish cyber and information security strategy	01/05/2018	Inconsistent	IHL applies in cyberspace and distinction must be made between civ and mil object. But not explicit on 'data' as an object, unclear whether can *assume* that this follows from the fact that principle of distinction applies.	Increased vulnerability of infrastructure. Critical infrastructures: energy, healthcare, transport, telecom, financial sector, maritime sector, drinking water supply, domain name systems.
Denmark	Military Manual	01/01/2020	Negative	Digital data does not in general constitute an object under the principle of distinction.	/
Denmark	Danish Ministry of Defence: official statement	03/11/2022	Inconsistent	IHL applies in cyberspace and distinction must be made between civ and mil object.	Denmark's national strategy focusses on protection of State's critical it-systems.

				But not explicit on 'data' as an object, unclear whether can *assume* that this follows from the fact that principle of distinction applies.	
Denmark	Official statement after cyberattack on companies in the energy industry	08/12/2023	Inconsistent	Large attack on the data of the energy industry resulting in a physical disruption, but no comment on whether this attack on data was considered an attack on a civilian object.	Emphasises the attack being directed at critical infrastructure and hints towards the involvement of Polish and Russian hackers (IP-addresses).
Finland	Finland's cyber security strategy: official statement	08/05/2011	Inconsistent	IHL applies in cyberspace and distinction must be made between civ and mil object. But not explicit on 'data' as an object, unclear whether can *assume* that this follows from the fact that principle of distinction applies.	Need for international cooperation and increase confidence between states, but mostly on EU level. Believes EU is a central player. Key challenge is to find balance between the freedom and transparency of digital networks and their security.
Finland	Statement by Ambassador at the OEWG on developments in the field of information and telecommunications in the context of international security	10/02/2020	Inconsistent	IHL applies in cyberspace and distinction must be made between civ and mil object but not explicit on 'data' as an object, unclear whether can assume that this follows from the fact that principle of distinction applies. "*The unique characteristics of cyberspace, such as interconnectedness (…) affect the interpretation (…) of IHL with regard*	"*A rule-based international order is our best hope in tackling present and future global challenges, including in cyberspace*." "*New norms are possible, but should not create confusion with existing international law*".

				to cyber warfare. The related problems can nevertheless mostly be solved on the basis of existing rules."	
Finland	National position: contribution to the UN GGE	15/10/2020	Inconsistent	"*Cyber means and methods of warfare must be used consistently with the principles of distinction, (…), as well as the specific rules flowing from these principles. (…) Constant care shall be taken to ensure the protection of (…) civilian objects, including essential civilian infrastructure, civilian services and civilian data*."	It states that the principle of distinction applies, must be interpreted in the light of cyberspace and so also civilian data must be protected, but seems to look more at it as a separate type of distinction between civilian and military, rather than considering data a type of object.
Finland	National position on public international law in cyberspace	15/10/2020	Inconsistent	IHL applies in cyberspace, but not explicit on principle of distinction and 'data' as an object, unclear whether can *assume* that this follows from the fact that principle of distinction applies.	*"Nothing should be interpreted as undermining international law."*
Finland	Official Statement Ministry of Foreign Affairs	15/10/2020	Inconsistent	IHL applies in cyberspace, but not explicit on principle of distinction and 'data' as an object, unclear whether can *assume* that this follows from the fact that principle of distinction applies.	Cyberspace is not the wild west. Finland emphasises the importance of international law in cyberspace as a basis for in-depth discussions.
Finland	Government's Defence Report	09/09/2021	Inconsistent	IHL applies in cyberspace, but not explicit on	/

				principle of distinction and 'data' as an object, unclear whether can *assume* that this follows from the fact that principle of distinction applies.	
Finland	Finland's Statement: Open-Ended Working Group on ICTs in the Context of International Security	01/04/2022	Inconsistent	IHL applies in cyberspace, but not explicit on principle of distinction and 'data' as an object, unclear whether can *assume* that this follows from the fact that principle of distinction applies.	A further dialogue is necessary between stakeholders to foster a better understanding of the opportunities and challenges.
Finland	Official statement after cyberattack on the website of the Finnish government.	08/04/2022	Inconsistent	No further comments on whether the disruption of data was considered a disruption of a civilian object.	The Finnish governments stated that the attack happened during the speech of Ukraine's President Zelensky but did not mention anything of a potential suspect.
France	Ministry of Defence: White Paper on Defence and National Security	09/07/2008	Inconsistent	IHL applies in cyberspace and distinction must be made between civ and mil object. But not explicit on 'data' as an object, unclear whether can *assume* that this follows from the fact that principle of distinction applies.	Focus on protection of critical infrastructure
France	French Cyberdefence Policy	08/06/2012	Affirmative	The mere theft of digital data and encryption is considered a criminal offence. IHL and its principles apply and have to limit	/

				the use of cyberspace.	
France	Cyber Security Report	01/03/2017	Inconsistent	IHL applies but recognises difficulty in interpreting the principles of IHL in cyberspace.	Moved from a passive defense policy to an active and dynamic defense
France	Ministry of Defence: international law applicable to operations in cyberspace	12/11/2018	Affirmative	IL and IHL apply, including its cardinal principles, such as: non-intervention, distinction. "*Les cyber-opérations visent exlcusivement des infrastructures numériques identifiées comme objectifs militaires*." "*Une attaque menée dans le cyberspace ne peut être dirigée contre des systems informatiques utilises par des écoles, établissements médicaux, ou (…) tout autre service exclusivement civil. (…) Des données de contenu (données civiles, bancaires, médicales,…) sont protégées au titre du principe de distinction*." Not explicitly affirming it as being an object, but here it is definitely protected as one, because of the dependence of societies on digital info.	"*Le respect du droit international est, pour la France, une condition à l'émergence d'une regulation adaptée du cyberspace*". "*Les riques liés à l'emploi d'une cyber-arme (…), l'hyperconnectivité (…), exigent un processus de ciblage numérique spécifique encadrant l'ensemble des phases de la cyber-opération, ceci afin de les soumettre aux principles de distinction (…).*" Mentions as important civilian data: governmental data, banking data, and medical data.
France	Court of Appeal of Versailles, Fifth	03/12/2020	Negative	"*Elle fait l'objet d'une cyberattaque de Janvier à février*	/

	Chamber, *N° 19/00160*			*2020 ayant entrainé la perte de la majeure partie de ses archives*": not established that this was criminal conduct and that the data was protected.	
France	Statement: Open-Ended Working Group on IL applied to operations in cyberspace	14/07/2021	Affirmative	IHL applies in cyberspace and distinction must be made between civ and mil object. "*Given the current state of digital dependence, content data (such as civilian, bank or medical data etc.) are protected under the principle of distinction*."	'Content data' refers to the theory of Harrison-Dinnis that recognises two types of data: content data (mere information) and operational or program data (data used for the functioning of a system). When messed with the second type of data, there are inevitably physical effects. France's opinion suggests that this type of data is regarded at integral part of the infrastructure itself, whereas the content data is protected *an sich*.
France	Court of Appeal of Lyon, Eigth Chamber, *N° 20/0749*310	10/11/2021	Negative	"*Touchés par une cyberattaque qui a entrainé le cryptage des donées de l'entreprise*": not established that this was criminal conduct and that the data was protected	/
Germany	Federal Ministry of Defence: law of armed conflict: manual	01/05/2013	Inconsistent	IHL applies in cyberspace: for every principle (including distinction) a case-by-case assessment must be made to interpret the situation and see	/

				how the principle applies.	
Germany	Official statement after Bundestag Hack	01/05/2015	Inconsistent	The internal confidential communication data of the German authorities was stolen, but no comment on whether the theft of data was considered a theft of civilian objects.	German authorities pointed towards a Russian hacking group as the suspect, but only explicitly stated that the attack was launched by *"a foreign intelligence service"*.
Germany	Official Statement after cyber-attack against German government's network	18/03/2018	Inconsistent	IHL would apply if the attack would amount to an 'armed attack', including the principle of distinction, but does not mention whether the attack here falls under IHL.	Wants to avoid unnecessary escalation and conflict, did not want to answer all questions due to ongoing research on the attack and the culprit thereof. Sees a threat for international peace and security in the increased state sponsored and malicious cyber activity.
Germany	National position: contribution to the UN GGE	06/04/2020	Inconsistent	IHL applies in cyberspace and distinction must be made between civ and mil object. But not explicit on 'data' as an object, unclear whether can *assume* that this follows from the fact that principle of distinction applies.	Explicit objection against the need for a new legal framework. Essential infrastructures include: medical facilities and infrastructure essential to political processes and focus on the protection of these infrastructures.
Germany	National position on public international law in cyberspace	01/03/2021	Affirmative	"*A civilian object like a computer (…), or even data stocks (…)*."	*"The benchmark for the application of the principle of distinction is the effect caused by a cyberattack (…). Thus, computer viruses designed to spread their harmful effects*

					uncontrollably cannot distinguish properly between military and civilian (…) their use is therefore prohibited as an indiscriminate attack. In contrast, malware that spreads widely into civilian systems but damages only a specific military target does not violate the principle of distinction."
Germany	Ministry of Defence: position paper cyber operations	16/03/2021	Inconsistent	IHL applies in cyberspace and distinction must be made between civ and mil object. But not explicit on 'data' as an object, unclear whether can *assume* that this follows from the fact that principle of distinction applies.	/
Germany	LG Köln, 28 O 328/21	18/05/2022	Affirmative	If a cyber-attack results in the mere loss of data, including personal information this is a criminal offense and the victims must receive compensation.	/
Israel	Making of a new government agency: the National Cybernetic Taskforce	18/05/2011	Inconsistent	IHL applies in cyberspace and distinction must be made between civ and mil object. But not explicit on 'data' as an object, unclear whether can *assume* that this follows from the fact that principle of distinction applies.	Focus on protecting critical networks and R&D.

Israel	Comments on the draft report of the UN OEWG	01/04/2020	Inconsistent	IHL applies in cyberspace and distinction must be made between civ and mil object. But not explicit on 'data' as an object, unclear whether can *assume* that this follows from the fact that principle of distinction applies.	/
Israel	Official statement after cyberattack on Israel's water facilities	25/04/2020	Inconsistent	The attack targeted and disrupted the data of six water supply and treatment facilities on the regulation of chlorine and chemicals in the water. But no comment on whether the disruption of data was considered a disruption of a civilian object.	No explicit mention of a suspect but hinted towards Iran. Iran, however, denied all involvement. In May 2020, Iran suffered then a major cyberattack on data of the port computer system and Iran pointed at Israel for this attack. Israel never confirmed nor denied its involvement, but several other States saw a link between these two attacks. Potentially, this could be seen as a countermeasure.
Israel	Israel's perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations	09/12/2020	Negative	Existing IL and IHL suffices to regulate cyber operations and applies in cyberspace and distinction must be made between civ and mil object. However, only tangible objects can constitute objects and so data cannot be seen as an object possessing a military or civilian nature, but if an operation against	Sees itself as a technologically advanced state part of a group of mostly Western states. Israel early on felt incentivised to develop (cyber) military capabilities. Has been a major actor in cyber operations and aims to legitimise these under international law.

				data causes effects that qualify the operation as an attack (physical damage, injury), the IHL rules governing attacks would apply.	
Israel	Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations	01/01/2021	Negative	*"Objects for the purposes of LOAC have always been understood to be tangible things and this understanding is not domain-specific. It is therefore our position that, under the law of armed conflict, as it currently stands, only tangible things can constitute objects. (…) This does not mean that cyber operations adversely affecting computer data are unregulated. (…) When an operation involving the deletion or alteration of computer data is still reasonably expected to cause physical damage to objects or persons and fulfills the other elements required to constitute an attack, the operation would be subject to LOAC targeting rules."*	"*One must have regard to rules, which are not dependent on the concept of objects, such as the obligation to respect and protect medical units*."
Israel	Official Statement on the application of International Law to cyberspace	25/10/2021	Inconsistent	IHL applies in cyberspace and distinction must be made between civ and mil object. But not explicit on 'data' as an object, unclear whether	"*Particular attention needs to be afforded to the protection of government data stored by third-party cloud providers*."

				can *assume* that this follows from the fact that principle of distinction applies.	
New Zealand	Manual Law of Armed Conflict	07/08/2017	Inconsistent	IHL applies in cyberspace and distinction must be made between civ and mil object. But not explicit on 'data' as an object, unclear whether can *assume* that this follows from the fact that principle of distinction applies.	"*They are not to carry out cyberattacks that: (…) are directed against civilian objects, including computers, computer networks and cyber infrastructure, unless the become a military objective*." But data was not explicitly included in this list
New Zealand	National position: contribution to the UN GGE	01/02/2020	Inconsistent	IL and IHL apply in cyberspace and distinction must be made between civ and mil object. But not explicit on 'data' as an object, unclear whether can *assume* that this follows from the fact that principle of distinction applies.	*"New Zealand is particularly concerned about (…) the trend towards malicious compromises of mass personal data."*
New Zealand	Official Statement on the application of International Law to cyberspace	01/12/2020	Inconsistent	IHL applies in cyberspace and distinction must be made between civ and mil object. But not explicit on 'data' as an object, unclear whether can *assume* that this follows from the fact that principle of distinction applies.	New Zealand is one of the "Five-Eyes" (Australia, Canada, UK and US): states that cooperate and collaborate closely in these affairs.
New Zealand	High Court of New Zealand, *CIV-2021-485-379*	04/08/2021	Affirmative	Data as such stolen due to a cyberattack, which is recognised as a criminal activity.	/

New Zealand	High Court of New Zealand, *CIV-2020-404-000609*	02/03/2023	Affirmative	Data as such stolen due to a cyberattack, which is recognised as a criminal activity.	/
Norway	Norwegian Ministry of Defence: Manual on the law of armed conflict	19/03/2013	Inconsistent	IHL applies to cyberspace and distinction must be made between civ and mil object. But not explicit on 'data' as an object. "*Damage to or destruction of civilian data in connection with an attack against military cyber infrastructure will be equivalent to causing incidental damage, injury or loss by kinetic means*."	"*In (…) cyberattacks, this requirement presents a challenge and is an important factor in the legal assessment prior to and during a cyberattack*."
Norway	Oslo Manual on Select Topics of the Law of Armed Conflict	09/10/2020	Affirmative	"*There is an increasing legal debate as to whether intangible objects are to be considered property. The Group of Experts did not reject the possibility that, for example, data can qualify as "property" under LOAC*."	"*In or through cyberspace means that operations covered (…) include both those the effects of which are confined to cyberspace and those that have effects in the physical world through the manipulation, deletion or corruption of data*."
Norway	National position: contribution to the UN GGE	13/07/2021	Inconsistent	IHL applies to cyberspace and distinction must be made between civ and mil object. But not explicit on 'data' as an object, unclear whether can *assume* that this follows from the fact that principle of distinction applies.	"*Complying with IL is fundamental for preserving international peace and security in cyberspace*. "*Cyberattacks during armed conflicts are subject to the same restrictions and regulations under IHL as conventional attacks, including*

					the principles of (…) and distinction." "*IHL (…) prohibits destroying, removing or rendering useless objects indispensable to the survival of the population, including through cyber means and methods of warfare. Objects indispensable to the survival of the civilian population include ICT infrastructure for food production or drinking water installations*."
Norway	Official Statement on the application of International Law to cyberspace	04/07/2023	Inconsistent	IHL applies to cyberspace and distinction must be made between civ and mil object. But not explicit on 'data' as an object, unclear whether can *assume* that this follows from the fact that principle of distinction applies.	"*Attacks against civilians or civilian objects are for example prohibited*."
Romania	Romanian National Ministry of Defence: the military strategy of Romania	01/01/2016	Inconsistent	IHL applies to cyberspace, but not explicit on data as an object.	"*The critical civilian infrastructure objectives, as well as defense communications systems and information technology equipment may be probable targets* for such attacks."
Romania	Romanian statement: the security fears that keep European awake at night	01/07/2018	Inconsistent	IHL applies to cyberspace, but not explicit on data as an object.	*"The weakest links in any computer system – those that hackers are most likely to target- are usually accounts or*

					data held by private citizens."
Romania	Voluntary national contribution on the subject of how IL applies to the use of information and communications technologies by Romania submitted in the Group of Governmental Experts	13/07/2021	Affirmative	IHL and the principle of distinction apply*:* *"There are ongoing discussions in relation to qualifying data as an object (…). We take the preliminary view that cyber operations against data do trigger the application of IHL. Therefore cyber-attacks can only be directed against those data that represent military objectives according to IHL and cannot be directed against those data that represent a civilian object which must be protected under the principle of distinction."*	*"The full respect for the IL is one of the most important pillars of Romania's foreign policy."*
Switzerland	Report on the Security Policy	23/06/2010	Inconsistent	IHL applies to cyberspace and distinction must be made between civ and mil object. But not explicit on 'data' as an object, unclear whether can *assume* that this follows from the fact that principle of distinction applies.	Recognizing the importance of critical infrastructure and its vulnerability to cyberattack.
Switzerland	Law Manual of Air and Missile Warfare	01/03/2017	Inconsistent	IHL applies to cyberspace and distinction must be made between civ and mil object. But not explicit on 'data' as an object, unclear whether can *assume* that	/

				this follows from the fact that principle of distinction applies.	
Switzerland	National position: contribution to the UN GGE	09/04/2020	Inconsistent	IHL applies to cyberspace and distinction must be made between civ and mil object. But not explicit on 'data' as an object, unclear whether can *assume* that this follows from the fact that principle of distinction applies.	/
Switzerland	National position on public international law in cyberspace	18/03/2021	Inconsistent	IHL applies to cyberspace and distinction must be made between civ and mil object. But not explicit on 'data' as an object, unclear whether can *assume* that this follows from the fact that principle of distinction applies.	*"The question, how exactly data is protected in the absence of such physical damage, remains a challenge. In practice, a responsible actor should generally be able to assess the potential impact of their actions and any resulting damage. As this estimation depends, amongst other things, largely on the information available at the time when decisions about an operation are taken, the obligation to take all precautionary measures practically possible to spare civilians and civilian objects plays a particularly important role in the use of cyber means and methods of warfare."*
Switzerland	Official statement: maintaining	29/06/2021	Inconsistent	IHL applies to cyberspace and	/

	international peace and security in cyberspace			distinction must be made between civ and mil object. But not explicit on 'data' as an object, unclear whether can *assume* that this follows from the fact that principle of distinction applies.	
Switzerland	Official statement	10/03/2023	Inconsistent	IHL applies to cyberspace and distinction must be made between civ and mil object. But not explicit on 'data' as an object, unclear whether can *assume* that this follows from the fact that principle of distinction applies.	/
Switzerland	Official statement after cyberattacks	02/11/2023	Negative	No comment on whether disruption against civilian data was considered a disruption against a civilian object.	*"In addition to short-term operational disruptions as a result of data encryption, the publication of leaked business data causes consequential damage that is hard to quantify."*
United States	Cyberspace Review Policy	01/05/2011	Negative	"*(...) reserves <u>all</u> necessary means to defend itself and its allies and partners*".	Signed with Brazil in the same year a Defense Cooperation Agreement in which they join R&D and military exercises.
United States	US Department of State	18/12/2012	Inconsistent	IHL applies to cyberspace and distinction must be made between civ and mil object. But not explicit on 'data' as an object, unclear whether can assume that	*"The (...) principle of distinction applies to computer network attacks undertaken in the context of an armed conflict.* (…) *As in any form of armed conflict, the*

				this follows from the fact that principle of distinction applies.	*principle of distinction requires that the intended effect of the attack must be to harm a legitimate military t arget. We must distinguish military objectives – that is, objects that make an effective contribution to military action and whose destruction would offer a military advantage – from civilian objects, which under international law are generally protected from attack."*
United States	Official Report on the Tallinn Manual and US Cyber Policy	18/02/2013	Inconsistent	IHL applies to cyberspace and distinction must be made between civ and mil object. But not explicit on 'data' as an object, unclear whether can *assume* that this follows from the fact that principle of distinction applies.	*"In other words, this rule informs that the traditional, core principles of the law of war; namely, distinction, apply to cyber-attacks as they do for any attack. Cyber certainly predates the Tallinn Manual and cyber capabilities used in and during war also predates the Tallinn Manual. Nonetheless, US commanders and allies have been abiding by the LOAC even when using cyber tools to create kinetic-like effects. Indeed, the Tallinn Group has noted in Rule twenty that LOAC applies to cyber. Rule forty-nine then, is simply providing more, unneeded details, namely noting the principle of*

					distinction is also applicable to cyber."
United States	National position on public international law in cyberspace	01/04/2016	Inconsistent	IHL applies to cyberspace and distinction must be made between civ and mil object. But not explicit on 'data' as an object, unclear whether can *assume* that this follows from the fact that principle of distinction applies.	Emphasises to minimise civilian casualties.
United States	Cyberspace Operations Report	08/06/2018	Inconsistent	IHL applies to cyberspace and distinction must be made between civ and mil object. But not explicit on 'data' as an object, unclear whether can assume that this follows from the fact that principle of distinction applies.	/
United States	US Federal Court of Appeals for the Second Circuit, McMorris	01/04/2021	Inconsistent	Potentially (yet not explicitly) opening up to considering non-physical harm sufficient.	*"Plaintiffss usually have strong evidence that their data was stolen (…), but quite often they cannot say that all (…) of the data subjects had personally experienced fraudulent charges or identity theft. Instead, plaintiffs often allege that they face a risk of ID theft or other future harm from misuse of their data. The courts seemed to be warming to future harm as satisfying the injury-in-fact requirement."* *"Risk of future*

					harm: there must be solid allegations that the data stolen is very likely to be used for identity theft or other fraud."
United States	United States Court of Appeals, Sixth Circuit: Stockx Customer Data Security Breach Litigation	02/12/2021	Negative	Due to a cyberattack, the personal data of various customers was stolen and sold on the dark web, but no real-life consequences were found. The act was not considered criminal, the motion dismissed and the provider was not found liable.	/
United States	Legal Conference Cyber Warfare and the Law of Armed Conflict	18/04/2023	Inconsistent	IHL applies to cyberspace and distinction must be made between civ and mil object. But not explicit on 'data' as an object, unclear whether can assume that this follows from the fact that principle of distinction applies.	*"The U.S. government's involvement in an attack, or in defense of an attack, could involve seizing or blocking data or communications in ways that raise property, privacy or free speech issues. This could raise questions about what is justiciable and what degree of deference the courts will give to the government."*

ANNEX 6: SCHEME OF *OPINIO JURIS* AND STATE PRACTICE

The idea of annex 6 is to present a general scheme of the State practice and *opinio juris*. It presents the general view but refers to specific sources when these state particularities or deviate from the general approach that was found in the rest of the sources of a State. The remarks section presents certain particularities.

State	State practice	*Opinio juris*	Remarks
Australia	Awareness of potential effects, therefore: affirmative	Awareness of potential effects, therefore: affirmative	Critical infrastructure (telecom, finance, water, electricity, energy, gaz, government, IP, education, food, port, public transport, aviation, medical) needs additional protection.
Belgium	Affirmative	Affirmative	Most recent sources hint towards the consideration of the potential effects.
Brazil	Inconsistent: no explicit opinion on data as an object found.	Inconsistent: no explicit opinion on data as an object found.	Fear of merely copy-pasting current IHL rules in cyberspace and of a too Western approach. Therefore also keeps bonds with China and Russia who want new rules.
Chile	Inconsistent	Awareness of potential effects, therefore: affirmative	When confronted with an attack, no real comment or reaction: afraid of consequences or just uncertain?
Denmark	Negative: object is tangible	Negative: object is tangible	Critical infrastructure (energy) needs additional protection.
Finland	Awareness of potential effects, therefore: affirmative	Awareness of potential effects, therefore: affirmative	Specific concerns of the need for further international cooperation and

			dialogue on the subject.
France	Inconsistent: does not reflect OJ.	Awareness of potential effects, therefore: affirmative	Critical infrastructure (education, medical, governmental, finance) needs additional protection.
Germany	Most recent sources: awareness of potential effects, therefore: affirmative	Most recent sources: awareness of potential effects, therefore: affirmative	Critical infrastructure (medical and political) needs additional protection.
Israel	Negative: object is tangible	Negative: object is tangible or data-attack must result in physical secondary effects, "*as it currently stand*s".	Actively used attack on data against Iran itself in 2020. Critical infrastructure (R&D, medical, governmental) needs additional protection.
New Zealand	Affirmative	Awareness of potential effects, therefore: affirmative	Explicit mentions of fear of future potential harm against civilians through cyberspace.
Norway	Inconsistent: mentions the need for also secondary physical effects, but more recent sources are more concerned of the effects.	Inconsistent: mentions the need for also secondary physical effects, but more recent sources are more concerned of the effects.	Critical infrastructure (water- and food facilities) need additional protection.
Romania	Affirmative	Affirmative	Critical infrastructure (telecom) needs additional protection.
Switzerland	Inconsistent: no explicit opinion, but more recent sources are more concerned of the effects.	Inconsistent: no explicit opinion, but more recent sources are more concerned of the effects.	Critical infrastructure needs additional protection.
United States	Negative	Negative	Refers to potential harmful consequences for citizens, but uses this as a reason to want to attack data themselves.