State obligations in international cyber conflicts:

Fighting the vacuum of cyberspace

Ruben Verdoodt

Under scientific supervision of:
Prof.dr. J. Wouters

ABSTRACT

Cyber conflicts have been a popular subject in recent news and have gained particular academic attention by scholars. Nevertheless, key legal issues remain unresolved. The purpose of this paper is to address and discuss the acute legal questions that exist today. Just like the cyber operations it studies, it transverses different domains of international law. It starts off by analysing the state of affairs and the existing law-making initiatives. Next, it critically discusses the conditions under which, and the extent to which, a state may be held responsible for a cyber operation. Special attention is paid to the issue of non-state actors and the duty of due diligence.

Once it is established that a state can be held responsible, the paper delves into the obligations that a state bears. From this perspective, both peace-time and war-time cyber operations are covered, as well as their human rights implications. For peace-time operations, the scope is limited to violations of sovereignty, non-intervention and the use of force. These notions and their thresholds are briefly explored. For war-time operations, the paper deals with the international humanitarian law principles of distinction, proportionality and precaution. Specific attention is dedicated to issues of dual-use and data protection in armed conflict.

With regard to the human rights implications of an international cyber conflict, the paper analyses the interplay between international human rights law and international humanitarian law in cyber armed conflicts. It also makes an argument for a functional approach to jurisdiction for the purpose of the extraterritorial application of human rights instruments to cyber conflicts.

Before arriving at the final conclusion, the paper engages in a case study of the Israel – Iran cyber conflict. Here, the previous findings are put to the test.

1. INTRODUCTION

1.1. GENERAL INTRODUCTION

1. Situations of cyber conflict no longer belong to the realm of fiction. Practice has shown the growing popularity for states of deploying cyber tactics, launching cyber operations both as standalone operations and in combination with conventional warfare. By 2015, more than 100 states had established cyber units within their armed forces or agencies, a number that is definitely growing.[1] The reasons are clear. Cyber operations are seemingly not affected by any physical boundaries and can be launched nearly instantaneously and at a relatively low cost.[2] Compared to conventional means of warfare, there is a greater potential efficacity and a higher degree of precision possible.[3] Cyber operations also appear less violent and less dangerous to the civilian populations.[4]

2. Nevertheless, cyber operations can have grave consequences for individuals and their rights.[5] As the Stuxnet attack showed, cyber operations can even result in physical destruction.[6] The concern is elevated by the interconnected nature of cyberspace and the vulnerability of essential infrastructures.[7] In cyberspace, international humanitarian law issues of dual-use and spill-over risks are crucial. The threat of direct or excessive incidental harm to civilians is also real.[8] Very often, it proves to be technically challenging to find the origin of a cyber

---

[1] "Waging War in Peacetime: Cyber Attacks and International Norms", 20 October 2015, https://www.lowyinstitute.org/the-interpreter/waging-war-peacetime-cyber-attacks-and-international-norms, consulted on 5 May 2021; Geneva Internet Platform DigWatch, *UN GGE and OEWG*, https://dig.watch/processes/un-gge, consulted on 19 November 2021; ICRC, *Position Paper on International Humanitarian Law and Cyber Operations during Armed Conflicts, submitted to the OEWG and GGE*, 28 November 2019, 3, available at: https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts (hereafter: ICRC Position Paper).

[2] L. SWANSON, "The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict", *Loyola of Los Angeles International & Comparative Law Review* 2010, Vol.32(2), 304.

[3] D. DELIBASIS, "The Right of States to Use Force in Cyberspace: Defining the Rules of Engagement", *Information & Communication Technology Law*, 2002, Vol. 11(3), 257.

[4] For this reason, some authors contemplate whether cyber operations may even become an obligation under international humanitarian law, as opposed to physical operations: ICRC, *The Potential Human Cost of Cyber Operations*, ICRC Expert Meeting 14-16 November 2018, 36.

[5] ICRC, *The Potential Human Cost of Cyber Operations*, ICRC Expert Meeting 14-16 November 2018.

[6] Stuxnet is the name of the cyber worm that was used in a 2010 cyberattack against Iranian nuclear facilities. The worm was designed to sabotage the centrifuges of the nuclear facilities, making them spin at a high speed, causing the destruction of over 1.000 centrifuges: see e.g. "Iran, Victim of Cyber Warfare", 2015, https://casebook.icrc.org/case-study/iran-victim-cyber-warfare, consulted on 30 March 2021.

[7] For example, a power outage in a Dutch hosital caused the death of two patients: "Twee patiënten overleden na stroomstoring ziekenhuis Maastricht", 1 May 2021, https://nos.nl/artikel/2379029-twee-patienten-overleden-na-stroomstoring-ziekenhuis-maastricht, consulted on 5 May 2021; E. DIAMOND, "Applying International Humanitarian Law to Cyber Warfare" in P. S. BARUCH and A. KURZ (eds.), *Law and National Security: Selected Issues*, Institute for National Security Studies, 2014, 67, available at: https://www.jstor.org/stable/resrep08957.8.

[8] M.S. ISLAM, "Cyber Warfare and International Humanitarian Law: A Study", *International Journal of Ethics in Social Sciences* 2017, Vol.5(1), 107.

operation. This makes attribution very hard, if not impossible. For further complexification, states often rely on proxies to launch their cyber operations. Both legally and technically, attribution is a sore point. Some fear that such anonymity creates a risk of conflict escalation.[9] Cyber operations also entail a specific risk of proliferation, where the cyber tools used for an operation may leak and cause further unintended damage or be repurposed by other actors.[10] In addition to the above, states currently enjoy a legal grey zone for crucial aspects of their cyber operations.[11] Legal qualification of cyber operations is needed in order to ensure the rule of international law, to protect the rights of those involved and to avoid complete lawlessness of new types of conflict.

3. One might look to the grave physical consequences of the current Russo-Ukrainian conflict, where, besides some instances of cyber activity on both sides,[12] the feared large-scale cyber operations remain absent, and argue that cyber operations would have spared more lives.[13] While this may be true for a particular conflict, it may not be true for others, and it certainly is not an argument to allow malevolent states enjoying the legal grey zones around cyber operations. To make things more concrete and to show the acute nature of the legal challenges, this paper looks at the conflict between Israel and Iran that is currently being fought out in cyberspace. The idea for the subject of the paper originated from reading about this conflict. It shows the diversity of cyber operations being launched in an international cyber conflict and the threats that they pose to civilians and their rights. The goal is to distil abstract legal questions from the concrete set of facts, and to formulate an answer to these questions.

1.2. SCOPE AND METHODOLOGY

1.2.1. Scope and limitations

4. The main research question this paper seeks to answer is what obligations states bear in situations of international cyber conflict, such as they exist in practice. To answer this question, multiple sub-questions must be answered. First, how are cyber operations attributable to a state? If no attribution is possible, does a state have a due diligence obligation to prevent such operations from originating from within its territory? Second, which cyber operations is a state prohibited from conducting by international law? Third, can cyber

---

[9] ICRC, *Position Paper on International Humanitarian Law and Cyber Operations during Armed Conflicts*, 4.

[10] ICRC, *International Humanitarian Law and the Challenges of Contemporary Conflicts*, Geneva, 2019, 27, available at: https://shop.icrc.org/international-humanitarian-law-and-the-challenges-of-contemporary-armed-conflicts-recommitting-to-protection-in-armed-conflict-on-the-70th-anniversary-of-the-geneva-conventions-pdf-en.

[11] G. BROWN, "Why Iran didn't admit Stuxnet was an attack", *Joint Force Quarterly,* 2011, 63(4), 73: "*So far, the practice of States in cyberspace seems to be, 'do unto others whatever you can get away with*".

[12] For a convenient overview of the latest cyber operations in the conflict, see: https://www.cfr.org/blog/tracking-cyber-operations-and-actors-russia-ukraine-war.

[13] See for example the bombing of a television tower in Kyiv, which killed several civilians: https://www.reuters.com/world/ukraine-says-five-people-killed-russian-attack-kyiv-tv-tower-2022-03-01/.

operations by themselves create a cyber armed conflict, triggering the application of international humanitarian law (IHL)? If IHL applies, how are the principles of distinction, proportionality and precaution to be applied in cyberspace? Fourth, how are the human rights of individuals protected in situations of international cyber conflict?

5. It is important to flag that even though serious concerns may arise in the wide array of cyber operations, this research has a clearly defined limited scope. As the title suggests, the research is focused on obligations that states bear in situations of cyber conflict. The reason for analysing cyber conflicts from the perspective of state obligations is to be able to make a cross-section of the relevant domains of international law and to be able to address the most important legal challenges in this area today. Such a cross-section is necessary because practice shows that cyber operations rarely remain confined within one domain of the law. The pressing challenges include attribution, due diligence, principles of international humanitarian law (IHL) and extraterritorial application of human rights law.[14] This does mean that the paper covers a lot of ground. It has been attempted to be both concise and comprehensive on all fronts, careful not to breeze through dense topics, while making sure that particular attention is paid to explaining and discussing the most important issues.

6. The research is limited to what this author calls 'international cyber conflicts'. Essentially, this means that it looks at conflicts that arise in cyberspace between states whereby at least one state's obligations are triggered. An important limitation to the scope is that the issue of so-called transit-states is not dealt with.[15] The concept of an international cyber conflict is not to be equated with an international cyber armed conflict; to a certain degree, conflicts falling below the threshold of an armed conflict are also covered.[16] This is the case in so far the cyber operations amount to an internationally wrongful act. For this purpose, the paper studies the violations of sovereignty, non-intervention and the use of force. It may very well be that cyber operations violate certain specific treaty obligations of a state party, but this is not studied. It must also be emphasised that issues such as cybercrime, cyberterrorism, cybersecurity and information warfare fall outside the scope of this research.

7. The 'international' in international cyber conflict means that the scope is principally limited to inter-state conflicts. Thus, there is no focus on cyber conflicts that may arise between non-state actors, or between a non-state actor and a state. They are only treated from the perspective of state obligations, namely when the conduct of the non-state actor can be attributed to the state. This also means that the research does not cover non-international cyber armed

---

[14] "OEWG 2021-2025 1st substantive session", 17 December 2021, available at: https://dig.watch/events/un-oewg-2021-2025-1st-substantive-session/international-law.

[15] A transit-state is a state through which territory a particular cyber operation is being routed. It is a sensitive and important topic. While it may simplify the complex reality of cyber operations, its exclusion is necessary to keep the scope of the paper manageable.

[16] The distinction is relevant because an armed conflict enjoys its distinct legal regime, namely the law of armed conflict (or international humanitarian law or *ius in bello*).

conflicts, an area that is perhaps critically understudied. The concept of an international cyber conflict is in no way a legal one. It is the attempt of the author to formulate a concept that covers all situations of cyber conflict whereby at least two states are involved and in which state obligations are triggered – a description of situations as they exist in practice.

8. The focus on states obligations also means that remedial questions such as enforcement short of force or the right to self-defence are not studied. Procedural and evidence questions also fall outside the scope of the research. There is also no focus on the (international) criminal responsibility of non-state actors, individuals, nor of state agents in cyber armed conflicts. Finally, it deserves mentioning that the substantial study of IHL is largely limited to the rules relating to conflict qualification and the conduct of hostilities, and is not focused on specifically protected persons and objects.

1.2.2. Methodology

9. While describing the law is the logical first step in any legal research, the object of the paper is not simply descriptive, it aims to combine multiple approaches to study the research questions.[17] Given the cross-section character of the research, it was essential to first map out the legal regimes and notions that were to be crossed, before passing through them and dealing with them. The paper tries to do this in a structured manner, avoiding a sight-seeing tour past the must-see attractions. Even within the descriptive parts of the paper, it goes beyond a mere description (if this is even possible within international law). Rather, it sets out the different existing viewpoints on a particular issue, before engaging in the discussion itself. It is with these discussions that the paper aims to make a valuable contribution.[18] Sensible discussions cannot arise out of thin air but must be contextualised and substantiated.

10. An important part of the research consists of a defining and classifying research objective because it tries to place the phenomena under the existing legal framework.[19] This is also the reason why attention is paid to explicitly defining some important concepts. Legally qualifying and pigeon-holing the studied phenomena forms an essential part of the paper, in order to render existing international rules applicable to situations of cyber conflict.[20] The second main research objective of the paper is evaluative.[21] The paper examines whether the (potentially) applicable legal framework is effective and fit for purpose and

---

[17] L. KESTEMONT, *Handbook on Legal Methodology: From Objective to Method*, Mortsel, Intersentia, 2018, 9.
[18] L. KESTEMONT, *Handbook on Legal Methodology: From Objective to Method*, Mortsel, Intersentia, 2018, 10.
[19] L. KESTEMONT and P. SCHOUKENS, *Rechtswetenschappelijk Schrijven*, Leuven, Acco, 2017, 30; L. KESTEMONT, *Handbook on Legal Methodology: From Objective to Method*, Mortsel, Intersentia, 2018, 11.
[20] P. WESTERMAN and M. WISSINK, "Rechtsgeleerdheid als rechtswetenschap", *Nederlands Juristenblad*, 2008, 504.
[21] L. KESTEMONT and P. SCHOUKENS, *Rechtswetenschappelijk Scrijven*, Leuven, Acco, 2017, 32; L. KESTEMONT, *Handbook on Legal Methodology: From Objective to Method*, Mortsel, Intersentia, 2018, 17.

reviews whether the rules are apt to be applied in cyberspace or whether they need to be adapted. Evidently, because the paper engages in review of *lex lata* and in *de lege ferenda* discussions, it also has a recommendatory research objective.[22] This, however, does not have a general scope and is limited to certain specific issues on which the paper makes proposals. Finally, the paper has no research object of comparative law. The limited degree of comparative law analysis only serves the purpose of assessing state practice and *opinio iuris*, as well as evidencing geographical representation.

11. The paper relies on primary sources of international law.[23] Despite the lack of cyber-dedicated treaties, 'classic' treaties such as the 1969 Vienna Convention on the Law of Treaties, the 1945 Charter of the United Nations and the 1949 Geneva Conventions and their Additional Protocols have been consulted, as well as the main international human rights law Treaties, such as the 1950 European Convention for the Protection of Human Rights and Fundamental Freedoms and the 1966 International Covenant for Civil and Political Rights. Otherwise, the paper has relied on well-established rules of customary international law. To testify for their continued application to cyberspace, the paper has looked to expressions of *opinio iuris*, judgments of international tribunals, and comparative law analyses made by international organisations or doctrinal authors. It has itself also consulted and compared official state positions on cyber issues, in an attempt to verify and validate claims of customary status.

12. In addition, the research looks to the relevant case law. This includes judgments from the International Court of Justice, the European Court of Human Rights, the Human Rights Committee, the Inter-American Court of Human Rights, The International Criminal Tribunal for the former Yugoslavia (ICTY), the Iran – United States Claims Tribunal, as well as a few arbitral awards. The paper has also consulted a wide array of documents prepared by governments, expert bodies and international organisations. Because of the generally slow and diffident nature of state practice and *opinio iuris*, the paper draws heavily on the works of doctrinal authors for certain perhaps more controversial issues. Both online and offline sources have been consulted. Because of the intent to consult the most recent works, the majority of sources have been consulted in their online form, including for example European Journal of International Law blogposts. Attention is also paid to the geographical and ideological representation of doctrinal authors. While this was certainly not always possible, it has been attempted to include the visions of doctrinal authors active in the Global South.[24]

13. As set out earlier, the paper does not shy away from entering into *de lege ferenda* discussions, careful to review both pro and contra positions in doctrine. However, the goal of this research is not to make *de lege ferenda* policy

---

[22] L. KESTEMONT, *Handbook on Legal Methodology: From Objective to Method*, Mortsel, Intersentia, 2018, 17.
[23] Article 38 Statute of the International Court of Justice.
[24] This has also been attempted for discussing and analysing State practice and opinio iuris.

recommendations.[25] Rather, it seeks to formulate legal answers to legal questions. The paper also takes into account, albeit to a very small degree, non-legal analyses of engineers, data-scientists and other practitioners. The reason for this is to account for the technical reality and feasibility of certain specific issues. Finally, for the purpose of the case study, the paper has relied on multiple online sources, from news sources to NGO analyses.

14. Because of the technical aspects inherent in the research matter, and thus inevitably part of the research itself, and because of the wide area of issues covered in the research, it is useful to study a specific case to be able to see the wood for the trees. In this way, all the findings can be applied and understood in a real context. It will both sum up the research and establish the difficulty of applying the theory in real life. For this purpose, the paper will analyse the Israel – Iran cyber conflict. The analysis in the case study is limited to lex lata in so far as possible. Given the fact that even some of the most basic legal principles are not readily accepted as lex lata in cyberspace, a too strict position would leave most questions unanswered. For this reason, de lege ferenda arguments are explicitly entertained. However, the paper is cautious to mention diverging state views, certainly in the course of the case study. Furthermore, it is not the intention to review the Israel – Iran conflict as an in concreto case study, in the sense that it will make abstraction of the facts. This is necessary because not enough information is publicly available to make correct in concreto conclusions on the conflict. Rather, the facts are treated as abstract scenarios, used to apply and review the theory.

2. INTERNATIONAL CYBER CONFLICTS AND THE LAW

2.1. A LEGAL VACUUM?

15. It can no longer reasonably be denied that cyber conflicts are regulated by law.[26] The short answer would be that there simply is no legal vacuum. However, the current state of affairs concerning the applicable law is a dynamic one and not much consensus between states can be found.[27] States have voiced their objections against a specific treaty or other instrument.[28] This means that, in the absence of newly developing custom, the existing international legal framework

---

[25] For some interesting policy proposals, see for example: ICRC, *The Potential Human Cost of Cyber Operations*, ICRC Expert Meeting 14-16 November 2018, 39-42.

[26] E. DIAMOND, "Applying International Humanitarian Law to Cyber Warfare" in P. S. BARUCH and A. KURZ (eds.), *Law and National Security: Selected Issues*, Institute for National Security Studies, 2014, 80, available at: https://www.jstor.org/stable/resrep08957.8; C. DROEGE, "No legal vacuum in space", *ICRC interview*, 16 August 2011, available at: https://www.icrc.org/en/doc/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm.

[27] M. N. SCHMITT and L. VIHUL, "The Nature of International Law Cyber Norms" in A. M. OSULA and H. ROIGAS (eds.), *International Cyber Norms – Legal, Policy & Industry Perspectives*, Tallinn, NATO Cooperative Cyber Defence Centre of Excellence, 2016, 39.

[28] A. M. OSULA and H. ROIGAS (eds.), *International Cyber Norms- Legal, Policy & Industry Perspectives*, Tallinn, NATO Cooperative Cyber Defence Centre of Excellence, 2016, 14.

has to be resorted to in order to legally qualify situations of cyber conflict.[29] For example, in situations of cyber armed conflicts classic instruments such as the 1949 Geneva Conventions and their Additional Protocols would apply to completely new situations that could not even have been imagined at the time of their original drafting.[30] This may lead to legitimate concerns regarding the effectiveness and adaptability of such instruments in the context of cyberspace.[31] This shows that even if there were consensus on the applicable law, the real challenge emerges afterwards, in deciding on how the law applies concretely. In the meantime, this unclarity may be abused by malevolent states or other actors.

2.1.1. Potential applicable law

16. Given that this paper studies the obligations of states, evidently the law governing state responsibility and attribution under international law is relevant throughout the paper. In addition, general international law such as the law concerning sovereignty and the law of due diligence play an important role. To a lesser degree, the law of international peace and security is touched upon in relation to the issue of the sovereignty, non-intervention and use of force thresholds. For the second part, the law of armed conflict is the most prominent domain of law that is potentially applicable. For the purpose of this paper, it is useful to agree with the International Committee of the Red Cross (ICRC) in claiming that the terms "international humanitarian law" (IHL), "the law of armed conflict" and "*ius in bello*" are interchangeable.[32] Finally, taking into account the great potential of harmful consequences to civilians, both inside and outside the context of an armed conflict, the specialised regime of international human rights law is also highly relevant.

2.1.2. Initiatives

17. The lack of state consensus on what law applies and how does not correspond to a lack of concern with the issue of cyber operations. On the contrary, cyber operations are high on the agenda of the international community. For example, in 2013 a set of so-called confidence-building measures was adopted within the Organisation for Security and Co-operation in Europe.[33] The measures focus on cooperation and open communication and confirm the adherence to the principle of non-interference, to the sovereign right

---

[29] K. KITTICHAISAREE, "Public International Law of Cyber Space", *Law, Governance and Technology Series* 2017, Vol. 32, 1 and DOI: 10.1007/978-3-319-54657-5.

[30] Convention (I) for the Amelioration of the Condition of the Wounded and Sick in the Armed Forces in the Field of August 12 1949, *United Nations Treaty Series*, 75; Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) of 8 June 1977, *United Nations Treaty Series*, Vol. 1125, 3.

[31] N. MELZER, *Cyberwarfare and International Law*, UNIDIR Resources Paper, 2011, 36, available at: https://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf.

[32] N. MELZER, *International Humanitarian Law: A Comprehensive Introduction*, Geneva, International Committee of the Red Cross, 2019, 17.

[33] ORGANISATION FOR SECURITY AND CO-OPERATION IN EUROPE, Decision No. 1106: Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies, PC.DEC/1106, 3 December 2013, available at: https://www.osce.org/files/f/documents/d/1/109168.pdf.

of internet governance within a state's territory, and to international law and fundamental rights and freedoms in general. International humanitarian law is not mentioned in these measures. Civil society is engaged as well, with the prominent example of Microsoft proposing a 'Digital Geneva Convention'.[34]

18. Importantly, there have been attempts at clarification and cooperation within the framework of the United Nations (UN). On the one hand, there is the Group of Governmental Experts on advancing responsible state behaviour in cyberspace in the context of international security (GGE), which was established for the first time back in 2004. The GGE produced a rudimentary consensus report for the first time in 2010.[35] On the other hand, there is the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG), which convened for the first time in 2019. Both groups have as their mission to study how international law applies to the use of information and communication technologies by States.[36] The UN GGE is composed of experts appointed by 25 States. The OEWG has an open composition, allowing all interested UN Member States to join the discussion.

19. Commendable as it is, the process has been slow. In 2013, the GGE resulted in a final report which, in addition to non-binding norms and confidence-building measures, for the first time did affirm the applicability of international law, in particular the Charter of the United Nations, albeit only between 15 states.[37] The following session of the GGE failed to deliver a consensus report in 2017 because of disagreements on the applicability of IHL in cyberspace.[38] Such a setback shows the cautious attitude of states when it comes to recognising binding rules in cyberspace. On 28 May 2021, the GGE did succeed in publishing a final report.[39] The report confirms the applicability of international law and the UN Charter, now between all 25 participating states. The report further states that IHL only applies in scenarios of armed conflict, explaining that further study is necessary on how and when this applies to the use of ICTs by states.[40] The mandate for the GGE has been renewed until 2025. On its part,

---

[34] Microsoft, "A Digital Geneva Convention to Protect Cyberspace", *Microsoft Policy Papers*, available at: https://www.microsoft.com/en-us/cybersecurity/content-hub/a-digital-geneva-convention-to-protect-cyberspace.

[35] Geneva Internet Platform Digwatch, *UN OEWG and GGE*, available at: https://dig.watch/processes/un-gge.

[36] Resolution 73/27 of the General Assembly of the United Nations (5 December 2018), *UN Doc.* A/RES/73/27, 5; Resolution 73/266 of the General Assembly of the United Nations (22 December 2018), *UN Doc.* A/RES/73/266, 3.

[37] Report A/68/98 of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 24 June 2013, 2.

[38] S. SOESANTO and F. INCAU, "The UNGGE is dead: time to fall forward", European Council on Foreign Relations, *Commentary of 15 August 2017*, available at: https://ecfr.eu/article/commentary_time_to_fall_forward_on_cyber_governance/.

[39] Report A/76/135 of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, 14 July 2021.

[40] Report A/76/135 of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, 14 July 2021, 18.

the OEWG published its final report on 12 March 2021.[41] Interestingly, despite explicitly recognising humanitarian risks of cyber activities, no reference is made at all to IHL. The report only refers to responsible state behaviour and the applicability of international law, in particular the Charter of the United Nations.[42] It could perhaps be inferred that the reference to international law includes IHL, but it should be noted that multiple states were explicitly reluctant on its applicability and therefore its explicit inclusion.[43] The mandate for the OEWG has been renewed for 2021-2025.

20. Thus, it is clear that both the GGE and the OEWG remain inconclusive on the exact application of IHL and other domains in cyberspace. Once again, the issue is pushed forward for future studies and discussions. Interestingly, in the first substantive session of the 2021-2025 OEWG, the majority of the participating states agreed that the previous OEWG and GGE reports have confirmed that the existing international law, *including* IHL and human rights law, applies to cyberspace.[44] To sum up, while it has been noted that states generally adopt a 'policy of ambiguity and silence',[45] the seeming unwillingness of states must also not be exaggerated: the short history shows a growing consensus between states on the international law applicable in cyberspace.

21. Finally, one can look at a comprehensive attempt at international legal cooperation in this area, namely the production of the *Manual on the International Law Applicable to Cyber Warfare*, or the *Tallinn Manual* in short, supported by the NATO Cooperative Cyber Defence Centre of Excellence. In 2017, an updated version was published, the *Tallinn Manual 2.0.* The central question tackled in both editions of the Manual is whether the existing laws apply to cyber issues, and, if so, how. The first Manual had a limited scope, focusing mainly on cyber warfare, while the second edition also studies the law applicable in peacetime. The Manual has been drafted by an International Committee of Experts and consists both of commentary and interpretations, as well as rules adopted by consensus within the experts.[46] The authors of the Manual make clear that it is not an official document of NATO and that it should only be

---

[41] Report A/AC.290/20121/CRP.2 of the Open-ended working group on developments in the field of information and telecommunications in the context of international security, 10 March 2021, available at: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.

[42] Report A/AC.290/20121/CRP.2 of the Open-ended working group on developments in the field of information and telecommunications in the context of international security, 10 March 2021, 4-6, available at: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.

[43] Report A/AC.290/2021/CRP.3 of the Open-ended working group on developments in the field of information and telecommunications in the context of international security (Chair's Summary), 8-12 March 2021, para. 18.

[44] Geneva Internet Platform Digwatch, *UN OEWG ,* https://dig.watch/events/un-oewg-2021-2025-1st-substantive-session/international-law.

[45] D. EFRONY and Y. SHANY, "A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice", *The American Journal of International Law*, Vol. 112(4), 583-657; H. MOYNIHAN, *The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention*, Chatham House Research Paper, 2019, 10.

[46] M. N. SCHMITT (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge, Cambridge University Press, 2013, 6 (hereafter: Tallinn Manual 1.0).

understood as an expression of the opinion of the International Group of Experts as to the state of the law.[47] Furthermore, the Manual should not be read as a 'best practices' guide, since it claims to focus only on *lex lata,* and not on *de lege ferenda*.[48] Despite these caveats, the Manual proves to be quite useful. Since the rules adopted by consensus are based on customary international law or treaty law existing for the non-cyber counterparts, generally they would in principle be binding upon states in cyberspace.[49] Though, in the absence of a multilateral treaty or widespread formal acceptance, the global acceptance of the rules thus formulated remains questionable.[50]

22. At the least, the Tallinn Manual process is influential and provokes discussion, forcing opponents to argue why a certain existing rule would not apply in cyberspace, or why it would apply differently. To testify for its influence, the Tallinn Manual was for example used during the UN GGE process.[51] Moreover, most rules adopted by consensus are uncontroversial and take a cautious and conservative position.[52] However, states sometimes cherry-pick from the Manual or avoid referencing to it at all.[53] The recent report from the French ministry of defence on international law applied to cyber operations serves as an interesting counterexample. The report often explicitly mentions the Manual, both when agreeing and disagreeing with it.[54] It is noteworthy that France is only in disagreement with some majority positions expressed in the Tallinn Manual, and not with any of the consensus rules. France also offers more protection under IHL than the Tallinn Manual does (see *infra*, p. 59). The same is true for Germany's position.[55] But while the UK's position is similar, it is completely silent on the Tallinn Manual.[56] Within their contributions to the UN

---

[47] M. N. SCHMITT (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge*, Cambridge University Press, 2017, 2 (hereafter: Tallinn Manual 2.0).
[48] Tallinn Manual 2.0, 3.
[49] Tallinn Manual 2.0, 4.
[50] M. WATNEY, "Determining When Conduct in Cyberspace Constitutes Cyber Warfare in Terms of the International Law and Tallinn Manual on the International Law Applicable to Cyber Warfare: A Synopsis" in P. GLADYSHEV, A. MARRINGTON and I. BAGGILI (eds.), *Digital Forensics and Cyber Crime,* Moscow, Springer, 2014, 142 and DOI: 10.1007/978-3-319-14289-0_10; D. EFRONY and Y. SHANY, "A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice", *American Journal of International Law*, 2018, Vol. 112(4), 583-657.
[51] Tallinn Manual 2.0, 91 (footnote 152).
[52] M. N. SCHMITT, "The Notion of 'Objects' during Cyber Operations: A Riposte in Defence of Interpretive and Applicative Precision", *Israel Law Review* 2015, 48(1), 83.
[53] See e.g.: U.S. Department of Defense Cyber Strategy 2018, available at: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF; Ministry of Foreign Affairs of the People's Republic of China, *International Strategy of Cooperation on Cyberspace*, 2017, available at: https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/201703/t20170301_599869.html.
[54] Ministère des Armées, *Droit International Applique aux Operations dans le Cyberespace*, 2019, available at: https://www.justsecurity.org/wp-content/uploads/2019/09/droit-internat-appliqu%C3%A9-aux-op%C3%A9rations-cyberespace-france.pdf.
[55] German Federal Foreign Office and the German Federal Ministry of Defence, *Position Paper on the Application of International Law in Cyberspace*, March 2021, available at: https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf.
[56] United Kingdom Policy Paper, *Application of international law to state's conduct in cyberspace : UK statement*, 3 June 2021, available at: https://www.gov.uk/government/publications/application-

GGE, Germany, the Netherlands, Norway and Japan explicitly rely on the Tallinn Manual.[57] In a consultation of state views, the Inter-American Juridical Committee often relied on the Tallinn Manual as well.[58] Finally, for the second edition of the Manual, experts from over 50 states were consulted, alluding to at least some degree of diverse representation.[59]

23. To conclude, despite the lack of demonstrable widespread state consensus on some key rules of the Tallinn Manual, the rules relied upon in this research are generally reflective of customary international law.[60] Otherwise, the Manual's position is often used as the starting point, merely introducing the discussion and careful to consider critical voices.

2.2. INTERNATIONAL CYBER CONFLICTS

2.2.1. Introduction

24. An international cyber conflict exists whenever the rights of one state have been implicated by another state through cyber means, which is generally the case if an internationally wrongful act has been committed.[61] An internationally wrongful act exists when it is attributable to the state and constitutes a breach of an international obligation of the state.[62] Therefore, this chapter first studies the issue of attribution of state responsibility. Second, the chapter discusses a specific obligation that a state may bear: the due diligence obligation. Third, the chapter briefly looks at three core rights/obligations relevant to cyber conflicts: sovereignty, non-intervention and use of force. Note that everything that passes the threshold of an armed conflict is reserved for the next chapter (*infra*, p. 45).

---

of-international-law-to-states-conduct-in-cyberspace-uk-statement/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement.

[57] United Nationals General Assembly, "Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communication technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266", *A/76/136*, 13 July 2021.

[58] Inter-American Juridical Committee, *International Law and State Operations*, 2020, available at: http://www.oas.org/en/sla/iajc/docs/International_Law_and_State_Cyber_Operations_publication.pdf.

[59] CCDCOE, "Over 50 States Consult Tallinn Manual 2.0", 2 February 2016, available at: https://ccdcoe.org/news/2016/over-50-states-consult-tallinn-manual-2-0/.

[60] D. EFRONY and Y. SHANY, "A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice", *The American Journal of International Law*, Vol. 112(4), 583-657, 654.

[61] International Law Commission, Draft Articles on Responsibility for Internationally Wrongful Acts, *Yearbook of the International Law Commission*, 2001, vol. II, Part 2, 31-32 (paragraph 1-6 of the general commentary) (hereinafter: ILC, ARSIWA); ILC, ARSIWA, 34 (Article 2 and its commentary); A. COCO and T. D. S. DIAS, "'Cyber Due Diligence': A Patchwork of Protective Obligations in International Law", *European Journal of International Law*, 2021, 1-35, 15, and DOI: https://doi.org/10.1093/ejil/chab056.

[62] ILC, ARSIWA, 34 (Article 2).

2.2.2. Attribution of state responsibility

a. State responsibility in general

25. The idea of attribution of state responsibility is of cardinal importance to the international legal order: it ensures a strong commitment to existing international law and respect for the rule of law.[63] A state can be held responsible for internationally wrongful cyber acts, either when the state itself has committed the wrongful act or when responsibility for the act can be attributed to the state.[64] In principle, states do not incur legal responsibility for acts that do not breach international law obligations.[65] Below the use of force threshold, breaches may be in violation of a treaty, customary international law or general principles of law.[66]

26. For cyber operations, attribution of state responsibility proves to be particularly difficult, if not impossible.[67] This is due to technical possibilities to hide the identity and the origin of a certain cyber operation.[68] There is a disproportionality in the time dimension as well: while the attacker can perform a cyber operation nearly instantaneously, the victim is left with the time-consuming challenge of attribution. For example, only after a very long and thorough examination it was found that a cyberattack on Israel was conducted not by Iran but by China, due to complex techniques used in an attempt of deception.[69] Similarly, Russia's attack on South Korea's Winter Olympics of 2018 was using techniques that would point to North Korea or China as the culpable.[70] Even though an analysis of such techniques lies beyond the scope of this research, it evidences the need for a clear and apt framework for legal attribution of state responsibility.

27. The attribution of state responsibility is famously dealt with in the International Law Commission's (ILC) Draft Articles on Responsibility of states

---

[63] L. CHIRCOP, "A Due Diligence Standard of Attribution in Cyberspace", *International & Comparative Law Quarterly,* 2018, Vol. 67, 643-668, 643.
[64] Tallinn Manual 2.0, 84 (Rule 14).
[65] International Law Commission, Draft Articles on Responsibility for Internationally Wrongful Acts, *Yearbook of the International Law Commission* 2001, vol. II, Part 2, 31 (paragraph 4 of the General Commentary) (hereinafter: ILC, ARSIWA).
[66] Tallinn Manual 2.0, 84.
[67] H. LIN, "Cyber Conflict and International Humanitarian Law", *International Review of the Red Cross,* 2012, 886(94), 522.
[68] A. COCO and T. D. S. DIAS, "'Cyber Due Diligence': A Patchwork of Protective Obligations in International Law", *European Journal of International Law,* 2021, 1-35, 1-2, and DOI: https://doi.org/10.1093/ejil/chab056.
[69] "Chinese hackers disguised themselves as Iran to target Israel", 10 August 2021, https://www.technologyreview.com/2021/08/10/1031622/chinese-hackers-false-flag-iran-israel-fireeye/.
[70] "Chinese hackers disguised themselves as Iran to target Israel", 10 August 2021, https://www.technologyreview.com/2021/08/10/1031622/chinese-hackers-false-flag-iran-israel-fireeye/.

for Internationally Wrongful Acts (ARSIWA).[71] Because of widespread reliance by states and international courts, the ARSIWA is highly authoritative and largely recognised as reflective of customary international law.[72] It is unsurprising that the Tallinn Manual also heavily draws on the ARSIWA. The following sections will analyse the relevant rules on state responsibility, departing from the ARSIWA and its commentaries and as translated into cyberspace by the Tallinn Manual.

b. State organs

b.1. State organs sensu stricto

28. Article 4 ARSIWA and its commentaries state that the conduct of any organ of a state is attributable to that state. Per the Tallinn Manual, cyber operations conducted by organs of a state are attributable to the state.[73] A state cannot avoid responsibility by denying under its domestic law the entity its status as an organ of the state.[74] The rule concerns both *de iure* and *de facto* state organs. The latter are "*persons or groups who, while they do not have the legal status of state organs, in fact act under such strict control by the state*".[75] In its *Nicaragua* and *Bosnian Genocide* judgments, the International Court of Justice (ICJ) put forward a test of "*complete dependence on the state*".[76] If an entity fulfils this test, it can be equated with a state organ for the purpose of international responsibility. The ICJ made clear that such a qualification must remain exceptional, requiring a high degree of state control.[77] For example, state ownership alone does not suffice to equate a private entity with a state organ because it does not entail complete dependence.[78]

29. Importantly, the state incurs responsibility for any breach of international obligations, even if the conduct of the organ was *ultra vires* (exceeding the authority granted by the state or contravening its instructions).[79] This could be interpreted as a presumption that a state should be able to have oversight over its organs and their activities. If an organ acts or omits to act against instructions

---

[71] International Law Commission, "Draft Articles on Responsibility of States for Internationally Wrongful Acts, with commentaries", *Yearbook of the International Law Commission* 2001, Vol. II(2), 31-143 (hereinafter ILC, ARSIWA).
[72] G. HERNANDEZ, *International Law*, Oxford, Oxford University Press, 2019, 248.
[73] Tallinn Manual 2.0, 87 (Rule 15).
[74] ILC, ARSIWA, 42 (paragraph 11 of the commentary to art. 4); Tallinn Manual 2.0, 88.
[75] ICJ, Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia Herzegovina v. Serbia and Montenegro), Judgment, I.C.J. Reports 2007, paragraph 391.
[76] ICJ, Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Judgment, I.C.J. Reports 1986, paragraph 110 (hereinafter: ICJ, Nicaragua): the ICJ had to decide whether the acts of the contras, a rebel movement sponsored and trained by the U.S., could be attributed to the latter); ICJ, Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia Herzegovina v. Serbia and Montenegro), Judgment, I.C.J. Reports 2007, paragraph 392 (Hereinafter: ICJ, Bosnian Genocide): the ICJ had to decide whether acts of genocide by non-State actors could be attributed to the Former Republic of Yugoslavia.
[77] ICJ, Bosnian Genocide, paragraph 393.
[78] Tallinn Manual 2.0, 88.
[79] ILC, ARSIWA, 45 (article 7); Tallinn Manual 2.0, 89.

or outside granted authority, the state ought to be aware of this and should be the one bearing the consequences. Nevertheless, the ratio of attribution for state organs only holds true in so far the organ is acting in an apparently official capacity or under so-called 'colour of authority'.[80] In other words, this has to be distinguished from purely private actions or omissions committed by the organ for private gain. In the latter scenario, no attribution of state responsibility is possible.

b.2. Governmental authority

30. Article 5 ARSIWA concerns attribution of state responsibility for the conduct of persons or entities empowered to exercise elements of governmental authority.[81] The Tallinn Manual applied this to cyber conduct, integrated in its rule on state organs.[82] Such empowerment by the state can be done through legislative and administrative acts, but also contractually.[83] The exact scope and content of 'governmental authority' is not always clear and has to be assessed in each case. It generally refers to quintessential governmental functions.[84] The Commentary to the ARSIWA lists examples, such as the power of detention, the powers in relation to immigration control, or even police powers held by a railway company.[85]

31. In the scenario of a private actor being given governmental authority to conduct cyber operations, there is no need to show that the conduct was carried out under the control of the state (*infra*, p. 19).[86] It is generally accepted that the capacity and permission to conduct offensive military operations for the state would qualify as exercising an element of governmental authority.[87] Indeed, if 'waging war' against another state is not an act that is reserved for governmental authority, then what is? If a state delegates governmental authority, it cannot be done in secret and publicly denied: even if the empowerment happens contractually, there still needs to be a "*general legislative or other legal framework*" that allows for the delegation of powers.[88] In the context of cyber

[80] ILC, ARSIWA, 42 (paragraph 13 of the commentary to art. 4); Tallinn Manual 2.0, 89.
[81] ILC, ARSIWA, 42 (art. 5).
[82] Tallinn Manual 2.0, 87-89.
[83] H. TONKIN, *State Control over Private Military and Security Companies in Armed Conflict*¸ Cambridge, Cambridge University Press, 2012, 103; Tallinn Manual 2.0, 89.
[84] Tallinn Manual 2.0, 89.
[85] ILC, ARSIWA, 43 (Commentary to article 5, paragraph 2).
[86] ILC, ARSIWA, 43 (Commentary to article 5, paragraph 7).
[87] C. BEAUCILLON, J. FERNANDEZ and H. RASPAIL, "State Responsibility for Conduct of Private Military and Security Companies violating ius ad bellum" in F. FRANCIONI and N RONZITTI (eds.), *War by Contract: Human Rights, Humanitarian Law, and Private Contractors*, Oxford, Oxford University Press, 2011, 396-420, 404; H. TONKIN, *State Control over Private Military and Security Companies in Armed Conflict*¸ Cambridge, Cambridge University Press, 2012, 101; C. LEHNARDT, "Private military companies and state responsibility" in S. CHESTERMAN and C. LEHNARDT (eds.), *From Mercenaries to Market: The Rise and Regulation of Private Military Companies*, Oxford, Oxford University Press, 2007, 139-157, 147-148.
[88] H. TONKIN, "State Control over Private Military and Security Companies in Armed Conflict"¸ Cambridge, *Cambridge University Press*, 2012, 111; C. BEAUCILLON, J. FERNANDEZ and H. RASPAIL, "State Responsibility for Conduct of Private Military and Security Companies violating

armed conflicts, non-state actors may qualify as so-called Private Military and Security Companies (PMSCs) under this rule (*infra* p. 49).

32. It must be noted that the attribution of state responsibility only occurs here when the entity in question is acting in the empowered capacity, meaning that the acts in question are of a governmental character and that the entity is empowered by the state to carry them out.[89] Thus, states do not bear responsibility for just any act committed by such entities. However, the state does still bear responsibility for *ultra vires* acts that generally fall within the scope of their duties.[90] This is the case for example when acts are incidental to the main tasks given, in so far as they remain inside the state's grant of authority.[91]

33. Finally, for the sake of completeness but less relevant to this research, there is also a possibility for state attribution if the state is unable to exercise its governmental authority and a private actor temporarily steps in to exercise aspects of state authority, not dissimilar to the notion of *levée en masse* under international humanitarian law.[92]

b.3. Governmental assets

34. Traditionally, there is the rebuttable presumption – but nearly irrefutable – of attribution of state responsibility in case of the use of governmental assets, such as military equipment. The *ratio legis* is that private use of governmental assets without state involvement is highly unlikely. The Tallinn Manual argues that this logic cannot easily be translated into a cyber context, since the improbability of the private use of governmental assets is much less prevalent in cyberspace.[93] It is conceivable that another state or non-state actor is able to gain control over the governmental cyber infrastructure of a state to use it to conduct cyber operations.[94] Thus, it is argued that the use of governmental cyber infrastructure *an sich* is insufficient to attribute state responsibility.[95] Arguably, the same goes for a territorial argument, referring to the use of private cyber infrastructure located on the territory of a state, as an indication of the state's involvement in the operation.[96] For the latter issue however, the due diligence obligation of the territorial state is relevant (*infra*, p. 29).

---

ius ad bellum" in F. FRANCIONI and N RONZITTI (eds.), *War by Contract: Human Rights, Humanitarian Law, and Private Contractors*, Oxford, Oxford University Press, 2011, 396-420, 404.

[89] Tallinn Manual 2.0, 90.

[90] ILC, ARSIWA, 45 (art. 7); H. TONKIN, *State Control over Private Military and Security Companies in Armed Conflict*, Cambridge, Cambridge University Press, 2012, 113; Tallinn Manual 2.0, 90.

[91] Tallinn Manual 2.0, 90-91.

[92] ILC, ARWISA, 49; Tallinn Manual 2.0, 92.

[93] Tallinn Manual 2.0, 91.

[94] Tallinn Manual 2.0, 91.

[95] Report A/70/174 of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, 22 July 2015, 13 (paragraph 28(f); Tallinn Manual 2.0, 91.

[96] Tallinn Manual 2.0, 91-92.

c. Non-state actors

35. Per article 8 ARSIWA and its commentaries, a state can, in certain well-defined cases, be held responsible for the cyber operations of a non-state actor.[97] Non-state actors may be both individuals or groups. Certainly because of the general accessibility of cyber technology, the question of cyber operations by non-State actors is highly relevant.[98] Practice also shows that states rely on non-state actors to conduct their cyber operations.[99] As difficult as it is to reveal the origin of a certain attack in cyberspace, the more difficult it is to establish a connection with a state actor.[100] Per the ARSIWA and its commentaries, cyber operations conducted by non-state actors shall be considered an act of the state if the non-state actor is acting on the instructions of, or under the direction or control of, the state.[101] Despite the heading of article 8 ARSIWA ('conduct directed or controlled by a state'), this rule has created two different tests of state responsibility. The first test is that of instructions by the state to the non-state actor. The second is that of conduct of the non-state actor under the direction or control of the state. For clarity, these scenarios must be distinguished from the 'strict control' test dealt with earlier in the context of *de facto* state organs. The distinction is crucial for *ultra vires* acts (*infra*, p. 27). In addition to these two tests, per article 11 ARSIWA, a state may also be held responsible for the acts of non-state actors if it 'acknowledges or adopts' their acts (*infra*, p. 27).

c.1. Instructions

36. The first scenario is perhaps the clearest one of the two, although the ILC is not very consistent with its language in the ARSIWA, mixing terms such as 'instructions', 'specific instructions', 'directions' and 'authorisation'.[102] Simply put, the state must instruct the non-state actor to behave in violation with international law.[103] Some argue that the ARSIWA commentary suggests that a general instruction, which leaves open the method of fulfilling the instruction, suffices.[104] The ICJ, however, decided in *Bosnian Genocide* that the instructions must have been given in respect of each operation, not merely generally in respect of the overall actions taken by the non-state actors.[105] According to the Tallinn Manual, 'giving instructions' refers to the situation in which a non-state

---

[97] ILC, ARSIWA, 47 (article 8).
[98] E.T. JENSEN, "Due Diligence in Cyber Activities" in H. KRIEGER, A. PETERS and L. KREUZER (eds.), *Due Diligence in the International Legal Order*, Oxford, Oxford University Press, 2020, 252-269, 255.
[99] See for example the U.K. analysis of all cyber actors linked to the Russian State, available at: https://www.gov.uk/government/publications/russias-fsb-malign-cyber-activity-factsheet/russias-fsb-malign-activity-factsheet; see also the case study (*infra*, p. 79).
[100] ICRC, "Position Paper on International Humanitarian Law and Cyber Operations during Armed Conflicts", 8.
[101] ILC, ARSIWA, 47 (art. 8); Tallinn Manual 2.0, 95.
[102] ILC, ARSIWA, 48.
[103] H. TONKIN, *State Control over Private Military and Security Companies in Armed Conflict*, Cambridge, Cambridge University Press, 2012, 114.
[104] J. CRAWFORD, *State Responsibility*, Cambridge, Cambridge University Press, 2013, 145.
[105] ICJ, *Bosnian Genocide*, paragraph 208.

actor functions as a state's auxiliary.[106] This would be the case when for example a private entity is requested by the state, or by its armed forces, to conduct cyber operations. It has to be distinguished from the scenario dealt with earlier, in which a non-state actor is empowered by the state to exercise elements of governmental authority. Admittedly, the distinction is not always very clear, given that such empowerment can happen contractually. If a situation wherein a private actor conducts, at the request of the state, offensive cyber operations against another state does not qualify as an exercise of governmental authority of that state, the situation arguably still qualifies as an 'instruction' for the purpose of state responsibility, with a nuance for *ultra vires* acts (*infra*, p. 27).

c.2. Direction or control

37. The second scenario where the state can be held responsible for the acts of a non-state actor is where the latter is acting under the direction or control of the state. The conditions 'direction or control' are most often interpreted conjunctively as referring to a continuing process of exercising authority over an activity, despite the ARSIWA intending them to be disjunctive.[107] Per the commentaries, a cyber operation launched by a non-state actor is attributable to the state if that state directed and controlled the specific operation and the conduct complained of forms an integral part of that operation.[108] This is not the case with mere state ownership (*supra*, p. 16), nor with general support or encouragement by the state.[109]

38. How the test must be understood has famously been the subject of debate. One approach is that of 'effective control', originally put forward by the ICJ in *Nicaragua*.[110] Another approach is that of 'overall control', created by the ICTY in *Tadic*.[111] The ARSIWA commentary itself discusses both these approaches.[112] Nevertheless, ever since the ICJ struck down 'overall control' and upheld 'effective control' for the purpose of attribution in *Bosnian Genocide*, it is generally accepted that the 'effective control' doctrine is applicable to decide on attribution.[113] Under 'effective control', the "*preponderant or decisive participation in the financing, organising, training, supplying, equipping, and planning the whole of the non-state actor's operation*" is insufficient to establish attribution of responsibility to the state.[114] Clearly, this is a high threshold. To

[106] Tallinn Manual 2.0, 95.
[107] Tallinn Manual 2.0, 96; J. CRAWFORD, *State Responsibility*, Cambridge, Cambridge University Press, 2013, 146; ILC, ARSIWA, 48 (article 8, paragraph 7).
[108] ILC, ARSIWA, 47 (paragraph 3 of the commentary to art.8).
[109] M. N. SCHMITT and L. VIHUL, "Proxy Wars in Cyberspace: The Evolving International Law of Attribution", *Fletcher Security Review* 2014, Vol. 1(2), 62; Tallinn Manual 2.0, 97.
[110] ILC, ARSIWA, 47-48 (paragraphs 4 to art. 8); ICJ, *Nicaragua*, paragraph 110.
[111] ICTY, *Tadic* (Appeals Judgment), IT-94-1-A, 15 July 1999, paragraph 137: "*The control required by international law may be deemed to exist when a State (...) has a role in organising, coordinating or planning the military actions of the military group, in addition to financing, training and equipping or providing operational support to that group*".
[112] ILC, ARSIWA, 47-48 (paragraph 4-5 of the commentary to art.8).
[113] ILC, ARSIWA, 47-48 (paragraphs 4 to art. 8); ICJ, *Nicaragua*, paragraph 110; ICJ, *Bosnian Genocide*, paragraph 392.
[114] ICJ, *Nicaragua*, paragraph 115.

date, it has never been met to find a state responsible.[115] Certainly in cyberspace, it seems unlikely that the use of proxies will ever meet this threshold. Indeed, a state providing malware to a non-state actor does not amount in and of itself to effective control over the operations by that non-state actor using the malware.[116] Nor would for example the scenario in which the state is financing the cyber operations conducted by the non-state actor, nor where the state is involved in planning the operation. Even the combination of the previous three examples would not meet the threshold of effective control. It can be noted that such actions, though insufficient to establish effective control for the purpose of attribution, might constitute a prohibited intervention or a use of force by the state (*infra*, p. 38).[117]

39. A critical analysis of 'effective control' in cyberspace has been made by multiple authors. According to some, the application of 'effective control' to cyberspace leads to attribution asymmetry because it makes the position of the victim state more difficult while allowing the responsible state to hide behind the non-state actor, yet still in a position to control the cyber operations.[118] Subsequent recourse by the victim state to the plea of necessity may risk further escalating the conflict.[119] More generally, some argue for a differentiated approach to 'control', instead of a strict and uniform standard of 'effective control' that applies equally in all contexts.[120] It is argued that the ILC in ARSIWA speaks of 'control' without further qualification, in combination with a commentary that suggests a flexible approach, meaning that additional rules may be formulated to account for new contexts.[121] In addition, article 55 ARSIWA provides for the possibility of a *lex specialis* "*where and to the extent that the conditions for the existence of an internationally wrongful act or its consequences are determined by special rules of international law*".[122] Thus, special regimes may have their own rules on attribution of responsibility.[123] For example, the United Nations Convention on the Law of the Sea contains a specific regime, where in certain circumstances state sponsorship of a private

---

[115] G. HERNANDEZ, *International Law*, Oxford, Oxford University Press, 2019, 256.
[116] Tallinn Manual 2.0, 97.
[117] Tallinn Manual 2.0, 97.
[118] K. KITTICHAISAREE, "Public International Law of Cyber Space" in *Law, Governance and Technology Series* 2017, Vol. 32, 42 and DOI: 10.1007/978-3-319-54657-5; P. MARGULIES, "Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility", *Melbourne Journal of International Law* 2013, Vol. 14, 1-24, 5.
[119] P. A. BANIS and M. V. ILYASHEVICH, "Due Diligence in the Digital Era: Question of Attribution of International Responsibility to a State" in E. POPKOVA and B. SERGI (eds.), *Artificial Intelligence: Anthropogenic Nature vs. Social Origin. ISC Conference - Volgograd 2020. Advances in Intelligent Systems and Computing*, Vol. 1100, Springer and https://doi-org.kuleuven.e-bronnen.be/10.1007/978-3-030-39319-9_35.
[120] N. TSAGOURIAS, "Cyberattacks, self-defence and the problem of attribution", *Journal of Conflict & Security Law* 17(2), 229-244, 238-239; F. DELERUE, *Cyber Operations and International Law*, Cambridge, Cambridge University Press, 2020, 144.
[121] ILC, ARSIWA, 47-49 (the ILC mentions both the ICJ *Nicaragua* 'effective control' approach and the ICTY *Tadic* 'overall control' approach); L. CHIRCOP, "A Due Diligence Standard of Attribution in Cyberspace", *International & Comparative Law Quarterly* 2018, Vol. 67, 643-668, 660.
[122] ILC, ARSIWA, 140 (paragraph 2 of the commentary to art. 55).
[123] N. TSAGOURIAS, "Cyberattacks, self-defence and the problem of attribution", *Journal of Conflict & Security Law* 17(2), 229-244, 239.

entity suffices for attribution of state responsibility.[124] Similarly, it can be argued that cyberspace may constitute a special regime requiring its own rules of attribution. Even if there is no agreement on this today, legally the scenario is not to be excluded.

40. One author argues that due diligence should be the standard for attribution of state responsibility in cyberspace (*infra*, p. 29 for a discussion on due diligence).[125] This would mean that if a victim state could point to a lack of due diligence on the part of the territorial state, attribution may be assumed, making that state potentially liable for the harm caused by the cyber operation.[126] For example, a lack of cooperation by the territorial state could be seen as a violation of the due diligence obligation, which would lead to the assumption of attribution.[127] Others argue for a concept of 'virtual control'.[128] In this perception, the findings in *Nicaragua* served as a rebuttable presumption, subject to evidence to the contrary, that the U.S. were not in control over the *contras*.[129] As such, under the concept of 'virtual control', the burden of proof would shift to the state that funds and equips the non-state actor, to demonstrate that it is not responsible for the cyber operations conducted by the non-state actor.[130] This is criticised, since it might lead to responsibility of unaware or incapable states that fail to rebut the presumption.[131] This author agrees with such critical views on effective control in cyberspace but is not convinced by the proposed 'due diligence' or 'virtual control' alternatives. In what follows, the author will discuss his view on the inaptitude of the effective control test for the attribution of cyber operations. The inaptitude is twofold.

41. First, the formulation is predicated on a kinetic situation. If "preponderant or decisive participation in the financing, organising, training, supplying, equipping, and planning the whole of the non-state actor's [cyber] operation"[132]

---

[124] Article 139 United Nations Convention on the Law of the Sea.
[125] L. CHIRCOP, "A Due Diligence Standard of Attribution in Cyberspace", *International & Comparative Law Quarterly* 2018, Vol. 67, 643-668, 668.
[126] L. CHIRCOP, "A Due Diligence Standard of Attribution in Cyberspace", *International & Comparative Law Quarterly* 2018, Vol. 67, 643-668, 648–649.
[127] E.T. JENSEN, "Due Diligence in Cyber Activities" in H. KRIEGER, A. PETERS and L. KREUZER (eds.), *Due Diligence in the International Legal Order*, Oxford, Oxford University Press, 2020, 252-269, 264.
[128] P. MARGULIES, "Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility", *Melbourne Journal of International Law*, Vol. 14, 496-519; K. KITTICHAISAREE, "Public International Law of Cyber Space", *Law, Governance and Technology Series* 2017, Vol. 32, 42-43 and DOI: 10.1007/978-3-319-54657-5; C. ANTONOPOULOS, "State Responsibility in Cyber Space" in N. TSAGOURIAS and R. BUCHAN (eds), *Research Handbook on International Law and Cyberspace*, Cheltenham, Edward Elgar, 2015; M. PIHELGAS, "Back-Tracing and Anonymity in Cyberspace" in K. ZIOLKOWSKI (ed.), *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy*, Tallinn, NATO CCD COE, 2013, 31-60.
[129] P. MARGULIES, "Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility", *Melbourne Journal of International Law*, Vol. 14, 509.
[130] K. KITTICHAISAREE, "Public International Law of Cyber Space", *Law, Governance and Technology Series* 2017, Vol. 32, 42 and DOI: 10.1007/978-3-319-54657-5.
[131] L. CHIRCOP, "A Due Diligence Standard of Attribution in Cyberspace", *International & Comparative Law Quarterly* 2018, Vol. 67, 643-668, 649.
[132] ICJ, *Nicaragua*, paragraph 115.

is insufficient to establish state responsibility, one may question what is left for the non-state actor to do. Indeed, all that is left to distinguish could be the theoretical push on a button by the non-state actor to launch the cyber operation. And where the Nicaragua logic served to prevent that the United States would have been held responsible for actions performed by the contras on the ground, where the United States itself were no longer directly involved and had no oversight, such a logic is absent in cyberspace (if only because there is no such physical operational ground). It is clear that the test is concerned with excluding situations where the state actor could not have exercised (sufficient) control for it to be held responsible: there must be a "real link" between the non-state actor and the state machinery.[133] Likewise, the ICTY in Tadic (Appeals Judgment) reasoned that the extent of control required decreases with the increasing proximity of the controlling state to the territory where the private conduct takes place.[134] Following this logic, one may accept that a state can be regarded as having more control over cyber operations conducted by non-state actors from within its territory, and in which it is involved, than would be expected in a traditional kinetic situation such as that in Nicaragua. In other words, there is no territory dividing (physically distancing) the state from the conduct of the non-state actor which would excuse the state's involvement up to the 'effective control' limit. Furthermore, effective control refers to the ability both to cause and to cease an activity. As established, states are in a much better position to cease cyber operations launched by non-state actors active on their territory, and in which they are involved, compared to an extraterritorial kinetic situation.

42. Second, the effective control test disregards the distinct nature of cyber operations from kinetic operations. Indeed, the means and methods of a certain cyber operation are predicated on the existence of a particular vulnerability in the targeted systems and are specifically designed to exploit these vulnerabilities.[135] Consider the following example: state A provides a private group B with guns. It can reasonably be accepted that state A cannot be held responsible for the killings performed by B in the territory of state C, given the lack of control by state A over the actions of B. This is the logic of *Nicaragua*. The situation is different, however, if state A develops a cyber worm that is specifically designed to infiltrate the governmental cyber infrastructure of state C and hands this worm over to a private group B, who uses it to attack that specific infrastructure. State A could have (should have) reasonably expected that this would have been the result. One may agree that the specialised and narrow-purpose nature of such a state-developed cyber worm makes its transfer to a non-state actor suspiciously close to an instruction (*supra*, p. 19).

43. Because of this inaptitude, a specialised regime of attribution is necessary. Indeed, with no justifying circumstances, drawing the line at 'effective control' becomes arbitrary. As introduced earlier, a distinct regime is also legally possible (*supra*, p. 22). As the ARSIWA commentaries put it, "*it is a matter for appreciation in each case whether particular conduct was or was not carried out*

[133] ILC, ARSIWA, 47 (paragraph 1 of the commentary to art.8).
[134] ICTY, *Tadic* (Appeals Judgment), IT-94-1-A, 15 July 1999, paragraph 138-140.
[135] See for example so-called "zero-day" exploits.

under the control of a state, to such an extent that the conduct controlled should be attributed to it".[136] The ICTY in *Tadic* also agreed that the required degree of control may vary according to the factual circumstances of each case.[137] It also deserves attention that other approaches to control have been undertaken by for example the European Court of Human Rights ('effective overall control') and the Iran-United States Claims Tribunal (having to prove a lack of control to rebut the presumption of state responsibility for insurgents).[138] Currently, at least some states hold the door open for a specialised regime in cyberspace.[139] It can also be noted that state practice on political attribution of cyber operations to states does not seem to rely on effective control terms, even when claiming violations of international law.[140]

44. Perhaps a notion of 'crucial control' or 'material control' is better suited to apply in situations of cyber conflict. This notion is influenced by the ICJ's reasoning in *Nicaragua* on why the violations of human rights law and international humanitarian law could not be attributed to the state: "*Such acts could well be committed by members of the contras without the control of the United States*".[141] Thus, there is an argument that attribution is possible if acts could *not* be committed without state control. Crucial control would englobe positive actions and support from the state without which the cyber operations launched by the non-state actor would be not be possible.[142] In other words, the positive actions of the state are *conditiones sine qua non* and form the "*real link*".[143] In the earlier example, state A would be held responsible because its development and transfer of the cyber worm is what made the cyber operation by the non-state actor possible: without the positive action of the state, that cyber operation could simply not have taken place. This author argues that a notion of crucial control is not incompatible with the current law and understanding of control. At least, it would amount to "*organising, coordinating or planning (...) in addition to financing, training and equipping or providing operational support to that group*", meeting the 'overall control' threshold.[144] Per the above quote of *Nicaragua*, it fits the logic behind 'effective control' as well. Even if one agrees with the definition of 'effective control' put forward by Judge Ago in his separate opinion to *Nicaragua*, namely that it involves specific instructions by the state to commit a particular act or to carry out a particular task on its behalf, then crucial

---

[136] ILC, ARSIWA, 48 (paragraphs 5 of the commentary to art. 8)
[137] ICTY, *Tadic* (Appeals Judgment), IT-94-1-A, 15 July 1999, paragraph 117.
[138] ECtHR, *Louizidou v Turkey,* No. 40/1993/435/514, 18 December 1996, paragraph 56; Iran-United States Claims Tribunal, *Kenneth P. Yeager v The Islamic Republic of Iran*, (Case No. 10199), Partial Award, 2 November 1987, paragraphs 43-45.
[139] See e.g. Inter-American Juridical Committee, *International Law and State Operations*, 2020, 40-42, available at: http://www.oas.org/en/sla/iajc/docs/International_Law_and_State_Cyber_Operations_publication.pdf.
[140] See e.g. UK National Cyber Security Centre, "Reckless campaign of cyber attacks by Russian military intelligence service exposed", 3 October 2018, available at: https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed; see also attribution in the case study (*infra*, p. 79).
[141] ICJ, *Nicaragua*, paragraph 115.
[142] This is not unlike regimes for civil and criminal responsibility that exist in certain civil law systems.
[143] ILC, ARSIWA, 47 (paragraph 1 of the commentary to art.8).
[144] ICTY, *Tadic* (Appeals Judgment), IT-94-1-A, 15 July 1999, paragraph 137.

control may very well equate to a level of control traditionally associated with 'effective control'.[145] This is to stress that 'crucial control' is not a lower threshold *per se* but that it is a different one, adapted to the reality of cyber operations and embedded in existing law. Under a crucial control test, states do not have to worry about bearing responsibility for acts over which they do not have control, for it requires their direct involvement. At the same time, the test prevents states from hiding behind the veil of non-state actors.

45. Two situations can be distinguished. First, the transfer ("*supplying*", "*equipping*") of narrow-purpose cyber means by a state to a non-state actor can, because of its similarity to an instruction, establish attribution, contrary to what the traditional formulation of 'effective control' test provides.[146] The narrow-purpose nature of cyber means may also justify a different temporal focus on control: if sufficient (crucial) control exists at the time of transfer, no further control at the time of the actual launch of the cyber operation is required. This is because at the moment of transfer, the state is reasonably aware of the exact consequences. Of course, this is taking into account the nuance of *ultra vires* acts (*infra*, p. 27), but it is presumed that, precisely because of the narrow-purpose nature, chances for unforeseeable *ultra vires* acts are slim. Second, if the state otherwise supports the non-state actor's conduct (by "*financing*" "*organising*", "*training*", or "*planning*") (everything but launching the operation itself), recourse can be made to the crucial control test.[147] In this regard, it may also be useful to be reminded of the presumption on the use of governmental assets (*supra*, p. 18).

c.3. Ultra vires acts

46. Contrary to both *de iure* and *de facto* state organs, *ultra vires* acts by non-state actors are generally not attributable to the state.[148] Conduct by a non-state actor is *ultra vires* when it is unrelated to the operations it was instructed to carry out: incidental conduct would still cause state responsibility.[149] This would cover conduct that is integral, meaning that it forms an essential part of the operation over which the state exercises control. As an example, collateral damage caused by a malware leak is attributable to the state if the malware attack launched by the non-state actor was under (effective/crucial) control of the state.[150] If this is the case, it is irrelevant whether the non-state actor disobeys or ignores the state's directions.[151]

---

[145] ICJ, *Nicaragua*, Separate Opinion of Judge Ago, paragraph 16, available at: https://www.icj-cij.org/public/files/case-related/70/070-19860627-JUD-01-05-EN.pdf.
[146] ICJ, *Nicaragua*, paragraph 115.
[147] ICJ, *Nicaragua*, paragraph 115.
[148] ILC, ARSIWA, 48 (paragraphs 6-8 of the commentary to art. 8) and 45 (art. 7).
[149] Tallinn Manual 2.0, 98.
[150] Tallinn Manual 2.0, 98.
[151] Tallinn Manual 2.0, 98; ILC, ARSIWA, 48 (paragraphs 6-8 of the commentary to art. 8).

c.4. Acknowledgment and adoption

47. Per article 11 ARSIWA, acts may be attributed to the state when the state acknowledges and adopts the operations of a non-state actor as its own.[152] The ICJ recognised this practice as customary international law in *Tehran Hostages*.[153] The conditions for acknowledgement and adoption are cumulative, they require more than mere endorsement or tacit approval, albeit not necessarily express endorsement: the line is somewhere in between.[154] Essentially, it means that the state acts as if the actions performed by the non-state actor were its own. Arguably, a failure to act against a certain operation by a non-state actor may be interpreted as acknowledgment and adoption by the state, or it may breach the state's due diligence obligation (*infra*, p. 29).

a. Proving attribution

48. The burden of proof of attribution is for the victim state that claims to have suffered an international wrongful act. There is no requirement such as in criminal law to establish responsibility beyond any reasonable doubt. The standard of proof remains quite high and is referred to as 'clear evidence'.[155] Absolute certainty, or at least the elimination of all possible alternatives, is not required.[156] Victim states have to act with reasonable certainty based on clear evidence.[157] Some conclude by looking at practice that the standards concerning the availability and probity of evidence in cases of cyberattacks would be rather lax, taking a more political approach of attribution.[158] This does not, however, equate to casual evidence or purely political inferences.[159] Indeed, such a flexible or lower standard of proof creates a risk for states that are unable, or that are unaware, to refute claims.[160]

---

[152] ILC, ARSIWA, 52 (art. 11); Tallinn Manual 2.0, Rule 17(b), 99.
[153] ICJ, *United States Diplomatic and Consular Staff in Tehran* (*United States v. Iran*), Judgment, *I.C.J Reports* 1980, paragraph 74: the Iranian government endorsed the acts of the non-State actors and perpetuated them, which lead to the ICJ treating them as acts of the State.
[154] ILC, ARSIWA, 52-53 (paragraphs 6-9 of the commentary to art. 11); Tallinn Manual, 99.
[155] ICJ, *Nicaragua*, paragraph 109.
[156] M. N. SCHMITT and L. VIHUL, "Proxy Wars in Cyberspace: The Evolving International Law of Attribution", *Fletcher Security Review* 2014, Vol. 1(2), 66.
[157] M. N. SCHMITT and L. VIHUL, "Proxy Wars in Cyberspace: The Evolving International Law of Attribution", *Fletcher Security Review* 2014, Vol. 1(2), 66.
[158] N. TSAGOURIAS, "Cyberattacks, self-defence and the problem of attribution", *Journal of Conflict & Security Law* 17(2), 229-244, 235; P. CORNISH, D. LIVINGSTONE, D. CLEMENTE and C. YORKE, *On Cyber Warfare, A Chatham House Report*, Royal Institute of International Affairs, 2012, 33, available at: https://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/r1110_cyberwarfare.pdf; For an overview of *opinio iuris* of standard of proof, see: P. ROGUSKI, "Application of International Law to Cyber Operations: A Comparative Analysis of State's Views", *The Hague Program for Cyber Norms Policy Brief*, 2020, 13-17.
[159] N. TSAGOURIAS, "Cyberattacks, self-defence and the problem of attribution", *Journal of Conflict & Security Law* 17(2), 229-244, 235.
[160] L. CHIRCOP, "A Due Diligence Standard of Attribution in Cyberspace", *International & Comparative Law Quarterly* 2018, Vol. 67, 643-668, 649.

49. Technical attribution of cyber operations is a very challenging and time-consuming exercise.[161] This is probably the most important non-legal challenge of cyber operations. In practice, attribution is based on all available sources of information, which for cyber operations includes technical signatures and forensics.[162] According to some, "*attribution is what states make of it*", suggesting that it is not an exact science.[163] The success of attribution also heavily depends on the technological advancement of the victim State.[164] In 2018 the UK and the Netherlands jointly and publicly attributed a series of cyber operations to the military intelligence service of Russia.[165] The UK, remarkably, explicitly called the operations a violation of international law.[166] It seems that in practice, attribution often goes together with individual criminal prosecution, instead of formally invoking state responsibility.[167]

b. Conclusion

50. States often rely on non-state actors to launch cyber operations. Because the other mechanisms for attribution either require a very heavy burden of proof on the part of the victim state (*de facto* organs and instructions), or require positive *ex post* actions by the state (acknowledgment and adoption), the 'direction or control' mechanism will in practice be the most important test for attribution of state responsibility for cyber operations. Therefore, it is important that a specialised cyber regime for the 'direction or control' test is put in place, in lieu of the inapt 'effective control' test. This paper has proposed an alternative 'crucial control' test or a resort to state instruction for certain situations.

2.2.3. Due diligence

a. A cyber due diligence?

a.1. Introducing due diligence

51. There is the possibility that if no attribution of state responsibility can be established, some degree of state responsibility still entails for acts by non-state

---

[161] See for example: "Chinese hackers disguised themselves as Iran to target Israel", 10 August 2021, https://www.technologyreview.com/2021/08/10/1031622/chinese-hackers-false-flag-iran-israel-fireeye/.
[162] H. LIN, "Cyber Conflict and International Humanitarian Law", *International Review of the Red Cross* 2012, 886(94), 522.
[163] T. RID and B. BUCHANAN, "Attributing Cyber Attacks", *The Journal of Strategic Studies* 2015, Vol.38, 4-37, 7.
[164] W. BANKS, "Cyber Attribution and State Responsibility", *International Law Studies* 2021, Vol. 97, 1039-1072, 1053.
[165] United Kingdom and The Netherlands, *Joint Statement from Prime Minister May and Prime Minister Rutte*, 4 October 2018, available at: https://www.gov.uk/government/news/joint-statement-from-prime-minister-may-and-prime-minister-rutte.
[166] UK National Cyber Security Centre, 'Reckless Campaign of Cyber Attacks by Russian Military Intelligence Service Exposed', 4 October 2018, available at: https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed.
[167] F. DELERUE, *Cyber Operations and International Law*, Cambridge University Press, Cambridge, 2020, 182-183.

actors because of a due diligence duty of the state.[168] There are three approaches to a duty of cyber due diligence. First, the ICJ famously stated in the *Corfu Channel* case that it is every state's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other states.[169] The ICJ has confirmed in *Armed Activities* that it is a general principle of international law.[170] Therefore, it can be applied to new situations, unless state practice or *opinio iuris* explicitly exclude it. Applied to cyberspace, such an obligation means that "*a state must, according to either its actual or constructive knowledge and in light of its technological capability, take measures as may be reasonably expected of it to prevent or stop its territory from being used by a cyberattacker to injure the rights of another state.*"[171] For this purpose, a states' territory encompasses any cyber infrastructure within the sovereign territory of the state.[172] Second, the Tallinn Manual agreed that a principle of due diligence applies in cyberspace, merging the *Corfu Channel* due diligence obligation with the *Trail Smelter* no-harm principle.[173] The *Trail Smelter* arbitral award related to cross-border environmental consequences and concluded that a state is under an obligation to prevent transboundary environmental harm that results in serious consequences.[174] Third, the insistence on norms of responsible state behaviour within the UN GGE and OEWG may allude to state acceptance of a cyber due diligence duty, but it is relevant to note that they refrained from a binding formulation.[175] According to the ILC, the due diligence obligation has a sector-specific nature to its application, meaning that states will understand their obligations differently depending on the sector in question.[176] Thus, despite a general acceptance of the existence of *some* due diligence obligation, precisely how the standard has to be applied is still subject to debate.[177] In general, no

---

[168] ICJ, *Corfu Channel Case*, Judgment, *I.C.J. Reports* 1949, 22.

[169] ICJ, *Corfu Channel Case*, Judgment, *I.C.J. Reports* 1949, 22: the ICJ decided that Albania was responsible for mines within its territorial waters it had not installed itself because it would have known of them and did not notify their existence.

[170] ICJ, *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)*, Judgment, *I.C.J. Reports* 2005, paragraph 162: the case concerned a complaint by the Democratic Republic of the Congo against Uganda, Burundi and Rwanda for acts of armed aggression on its territory.

[171] K. KITTICHAISAREE, "Public International Law of Cyber Space", *Law, Governance and Technology Series* 2017, Vol. 32, 40 and DOI: 10.1007/978-3-319-54657-5.

[172] Tallinn Manual 2.0, 32.

[173] Tallinn Manual 2.0, 30-31; T. DIAS and A. COCO, *Cyber due diligence in international law*, Oxford Institute for Ethics, Law and Armed Conflict, 134, available at: https://elac.web.ox.ac.uk/files/finalreport-bsg-elac-cyberduediligenceininternationallawpdf.

[174] Trail Smelter Arbitration (United States of America v. Canada), *Reports of International Arbitral Awards*, Vol. III, 1965 ("serious consequence" and "clear and convincing evidence") (the case concerned the complaint of the U.S. against Canada for the transboundary environmental consequences of a polluting factory which the latter had installed close to the border).

[175] Report A/76/135 of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, 14 July 2021, 10; Report A/AC.290/20121/CRP.2 of the Open-ended working group on developments in the field of information and telecommunications in the context of international security, 10 March 2021, available at: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.

[176] T. STEPHENS and D. FRENCH, *International Law Association Study Group on Due Diligence in International Law*, Second Report, 2016, 47.

[177] T. STEPHENS and D. FRENCH, *International Law Association Study Group on Due Diligence in International Law*, Second Report, 2016, 7.

widespread consensus can be found on the legal status, scope or content of a cyber due diligence obligation between states.[178]

The acceptance of a binding cyber due diligence obligation would increase the stability of the cyber environment and strengthen international peace and security.[179] Indeed, even where there is no 'smoking gun' that would legally justify treating the cyber operation as that of the state, the State may incur international responsibility.[180] It must be noted that the responsibility is limited to the breach of the due diligence obligation and that it does not include responsibility for the actual cyber operation conducted by the non-State actors which the State failed to prevent.[181] Breaching the due diligence duty constitutes an internationally wrongful act of its own.[182]

a.2. Requirements

52. There are two limits to the existence of a due diligence obligation: one of *de minimis*, meaning that a certain degree of harm has to be caused, and one of State knowledge.[183] The *de minimis* threshold differs between the classic due diligence principle (contrary to the rights of other States) and the no-harm principle (serious adverse consequences). Generally, the due diligence obligation applies when the cyber operation in question amounts to an internationally wrongful act if it were conducted by a State.[184] Indeed, the obligation is to protect within its territory the rights of other States.[185] If the rights of the victim State are not threatened, the obligation does not apply, even if the attack is significant.[186] The 2021 UN GGE report does not go into details on the requirements and duties of the application of the due diligence obligation.[187]

---

[178] E.T. JENSEN and S. WATTS, "Cyber Due Diligence", *Oklahoma Law Review* 2021, Vol. 73, 645-710, 694-695; Inter-American Juridical Committee (CJI), *Improving Transparancy, International Law and State Cyber Operations, Fourth Report*, 5 March 2020, 20, available at: http://www.oas.org/en/sla/iajc/docs/CJI_doc_603-20_rev1_corr1_eng.pdf; M. N. SCHMITT, "In Defense of Due Diligence in Cyberspace", *The Yale Law Journal Forum*, 2015, Vol. 125, 69 (Schmitt argues that due diligence is a general principle of international law, meaning that presumably the principle applies unless State practice or *opinion iuris* excludes it).

[179] E. T. JENSEN, "Due Diligence in Cyber Activities" in H. KRIEGER, A. PETERS and L. KREUZER (eds.), *Due Diligence in the International Legal Order*, Oxford, Oxford University Press, 2020, 252-269, 253.

[180] M. N. SCHMITT, "In Defence of Due Diligence in Cyberspace", *The Yale Law Journal Forum* 2015, Vol. 125, 80.

[181] E. O. OKWORI, "The Obligation of Due Diligence and Cyber-Attacks: Bridging the Gap Between Universal and Differential Approaches for States", *Ethiopian Yearbook of International Law* 2018, 205-242, 219.

[182] M. N. SCHMITT, "In Defence of Due Diligence in Cyberspace", *The Yale Law Journal Forum* 2015, Vol. 125, 79.

[183] K. KITTICHAISAREE, "Public International Law of Cyber Space", *Law, Governance and Technology Series* 2017, Vol. 32, 39 and DOI: 10.1007/978-3-319-54657-5.

[184] Tallinn Manual 2.0, 34.

[185] Island of Palmas Case (Netherlands v United States of America), Arbitral Award, 4 April 1928, *Reports of International Arbitral Awards*, vol. II, 829-871, 839.

[186] E. O. OKWORI, "The Obligation of Due Diligence and Cyber-Attacks: Bridging the Gap Between Universal and Differential Approaches for States", *Ethiopian Yearbook of International Law* 2018, 205-242, 219.

[187] Report A/76/135 of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, 14 July 2021, 10.

53. Per the Tallinn Manual view, due diligence applies to conduct of non-State actors resulting in 'serious adverse consequences' *and* affecting a right of the target State, even if it does not violate international law per se.[188] This would only include conduct that, if conducted by a State, would breach an obligation owed to the target State.[189] Even though the exact threshold of severity remains disputed,[190] the experts of the Tallinn Manual agreed that operations, if conducted by a State, would constitute a prohibited intervention or a violation of sovereignty, trigger due diligence. On the other hand, it is clear that inconvenience, minor disruption or negligible expense is insufficient to amount to "serious adverse consequences".[191] Harm must rise to such a level that it becomes a legitimate concern in inter-State relations, so minor inconveniences or denials of service would not suffice.[192] There is no requirement for physical damage to objects or injuries to individuals. For example, interference with the operation of critical infrastructure would entail due diligence.[193] To conclude, deciding on the level of severity is a very difficult exercise, one the experts of the Tallinn Manual could not solve unanimously. For further complexity, although most acts contrary to the rights of other States are internationally wrongful acts, the overlap is not complete.[194] The double threshold used by the Tallinn Manual is criticised as not being *lex lata* of the due diligence principle, which according to some does not require the actual occurrence of harmful consequences.[195] The Tallinn Manual is also ambiguous when it comes to the exact threshold which would trigger due diligence, further convoluting the issue.

54. State knowledge is the second important element for applying the due diligence obligation. The knowledge requirement includes both actual and constructive knowledge. A State is regarded as having knowledge if State organs are aware or if credible information is received.[196] In *Corfu Channel*, the ICJ decided that the State must have known of the operations, despite the State denying that it had any knowledge.[197] This is called 'constructive knowledge': a State breaches its due diligence obligation even if it is *de facto* unaware but objectively should have been aware.[198] In this context, proof may be drawn from inferences of fact and circumstantial evidence, in so far as they leave no room

---

[188] Tallinn Manual 2.0, 34-35.
[189] Tallinn Manual 2.0, 36.
[190] M. N. SCHMITT, "Grey Zones in the International Law of Cyberspace", *Yale Journal of International Law* 2017, Vol.42(2), 11-12.
[191] Tallinn Manual 2.0, 36-37.
[192] M. N. SCHMITT, "In Defence of Due Diligence in Cyberspace", *The Yale Law Journal Forum* 2015, Vol. 125, 76.
[193] Tallinn Manual 2.0, 38.
[194] A. COCO and T. D. S. DIAS, "'Cyber Due Diligence': A Patchwork of Protective Obligations in International Law", *European Journal of International Law* 2021, 1-35, 15, and DOI: https://doi.org/10.1093/ejil/chab056.
[195] F. DELERUE, *Cyber Operations and International Law*, Cambridge, Cambridge University Press, 2020, 365; E. T. JENSEN and S. WATTS, "Cyber Due Diligence", *Oklahoma Law Review* 2021, Vol. 73, 645-710, 697.
Tallinn Manual 2.0, 40.
[196] Tallinn Manual 2.0, 40.
[197] ICJ, Corfu Channel Case, Judgment, *I.C.J. Reports* 1949, 18.
[198] Tallinn Manual 2.0, 41.

for reasonable doubt.[199] For example, the use of governmental assets is a potential indicium for knowledge by the State. Some have critiqued this understanding of the knowledge requirement, since malintent States may abuse the high standard of knowledge to implement a policy of plausible deniability.[200] Indeed, any allegation is extremely difficult to prove. Therefore, some argue for a duty for the State to undertake reasonable precautionary knowledge building measures.[201] Preventive duties will be discussed in the next subsection (*infra* p. 35).

b. Due diligence duties

b.1. Extent of the duty

55. Once the requirements are fulfilled, the State must take all reasonably available measures to stop the cyber operation.[202] What is understood as reasonable measures always depends on the particular context and on the State's capacities.[203] Exercising the obligation cannot exceed the factual capabilities of the State, be it legal, financial or technological.[204] The obligation is largely understood to be one of conduct rather than result, requiring not much more than the best efforts from States, as there are no standards of adherence.[205] In *Bosnian Genocide*, the ICJ stated that it was an obligation of conduct, arguing that a State cannot be under an obligation to succeed under every circumstance.[206]

56. Thus, the obligation is limited to taking feasible measures to terminate the cyber operations.[207] Only if (the continuation of) a cyber operation is the result of the State's failure to exhaust reasonably available measures to terminate the cyber operations, the due diligence obligation is breached.[208] A context-driven analysis is necessary, specifically considering the capacity of the State and the specifics of the harmful operation, to decide what feasible measures a State must

---

[199] ICJ, Corfu Channel Case, Judgment, *I.C.J. Reports* 1949, 18; K. BANNELIER-CHRISTAKIS, "Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?", *Baltic Yearbook of International Law* 2014, Vol. 14, 23-39, 29.
[200] C. PATRICK, "Debugging the Tallinn Manual 2.0's Application of Due Diligence Principle to Cyber Operations", *Washington International Law Journal* 2019, Vol. 28(2), 581-604, 600.
[201] C. PATRICK, "Debugging the Tallinn Manual 2.0's Application of Due Diligence Principle to Cyber Operations", *Washington International Law Journal* 2019, Vol. 28(2), 581-604, 601.
[202] Tallinn Manual 2.0, 43.
[203] Tallinn Manual 2.0, 47.
[204] E. O. OKWORI, "The Obligation of Due Diligence and Cyber-Attacks: Bridging the Gap Between Universal and Differential Approaches for States", *Ethiopian Yearbook of International Law* 2018, 205-242, 205.
[205] E. O. OKWORI, "The Obligation of Due Diligence and Cyber-Attacks: Bridging the Gap Between Universal and Differential Approaches for States", *Ethiopian Yearbook of International Law* 2018, 205-242, 205.
[206] ICJ, *Bosnian Genocide*, paragraph 430.
[207] T. KOIVUROVA, "Due Diligence", *Max Planck Encyclopedia of Public International Law*, Oxford, Oxford University Press, 2010, paragraph 15; Tallinn Manual 2.0, 48.
[208] Tallinn Manual 2.0, 49.

perform.[209] Feasible measures are essentially the same as so-called "*readily available measures*" to terminate the operation, which have to be exhaust.[210]

57. Evidently, the level of due diligence expected from a technologically advanced State would be higher than that of a less technologically developed State.[211] For this reason, States with an extensive cyber infrastructure could be opposed to an idea of due diligence in cyberspace.[212] However, even if the State has the capabilities, it only has to take action in so far as it is reasonable and feasible.[213] States thus maintain a reasonably large *marge de manoeuvre*, which is limited by the duty to fulfil in good faith their international obligations.[214] Therefore, domestic issues generally cannot excuse bad faith non-compliance and States are expected to take appropriate steps towards progressively realising their international obligations.[215]

b.2. Prevention

58. A big debate revolves around the question whether the due diligence obligation imposes preventive duties upon the territorial State.[216] Based on a comparison with the ICJ *Bosnian Genocide* reasoning, the Tallinn Manual decided that the obligation extends to cyber operations that have not yet been launched, but where preparations are being made and a reasonable State would conclude that the operation will be carried out.[217] This would not entail an obligation to take general preventive measures.[218] Indeed, the standard of constructive knowledge does not require the State to monitor, but only to behave as a hypothetical reasonable State in the given circumstances.[219] The 2021 UN GGE report also concluded that preventive monitoring is not required.[220] On the

---

[209] C. PATRICK, "Debugging the Tallinn Manual 2.0's Application of Due Diligence Principle to Cyber Operations", *Washington International Law Journal* 2019, Vol. 28(2), 581-604, 590.
[210] C. PATRICK, "Debugging the Tallinn Manual 2.0's Application of Due Diligence Principle to Cyber Operations", *Washington International Law Journal* 2019, Vol. 28(2), 581-604, 594.
[211] A. COCO and T. D. S. DIAS, "'Cyber Due Diligence': A Patchwork of Protective Obligations in International Law", *European Journal of International Law* 2021, 1-35, 19, and DOI: https://doi.org/10.1093/ejil/chab056.
[212] M. N. SCHMITT, "In Defence of Due Diligence in Cyberspace", *The Yale Law Journal Forum* 2015, Vol. 125, 74.
[213] M. N. SCHMITT, "In Defence of Due Diligence in Cyberspace", *The Yale Law Journal Forum* 2015, Vol. 125, 74.
[214] Resolution of the UN General Assembly, Declaration on Principles of International law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations (24 Oct 1970). *UN.Doc.* A/RES/25/2625, Principle 7.
[215] E. O. OKWORI, "The Obligation of Due Diligence and Cyber-Attacks: Bridging the Gap Between Universal and Differential Approaches for States", *Ethiopian Yearbook of International Law* 2018, 205-242, 225.
[216] M. N. SCHMITT, "In Defence of Due Diligence in Cyberspace", *The Yale Law Journal Forum* 2015, Vol. 125, 75 (contra).
[217] ICJ, *Bosnian Genocide*, paragraph 431; Tallinn Manual 2.0, 43.
[218] Tallinn Manual 2.0, 44.
[219] C. PATRICK, "Debugging the Tallinn Manual 2.0's Application of Due Diligence Principle to Cyber Operations", *Washington International Law Journal* 2019, Vol. 28(2), 581-604, 593.
[220] Report A/76/135 of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, 14 July 2021, 10.

other hand, the ICJ found in *Pulp Mills* that the State was subject to a continuous obligation to monitor the environmental effects of the disputed operations.[221]

59. Some authors argue that given the instantaneous nature of a cyber operation, the due diligence duty in cyberspace should cover preventive obligations.[222] This would mean that there is a duty to monitor, and indirectly that there is no requirement for knowledge, actual or constructive, for the due diligence obligation to apply.[223] The authors claim that this would be beneficial for the territorial State as well, since it enhances the potential for discovery of cyber threats. As mentioned earlier, some have argued for a duty for the State to undertake reasonable precautionary knowledge building measures.[224] In this understanding, there are actually two preventive duties for the State: first preventing the operation from originating (e.g. by implementing laws and institutions[225]), then once it knows of the operation, preventing any harm from the operation. Otherwise, there would only be a minimalist notion of due diligence applicable to cyberspace, due to the lack of a duty to prevent or monitor, the high threshold of harm, and an absolute requirement of knowledge.[226]

60. A preventive understanding of the due diligence obligation is not without risks.[227] First, preventive obligations may interfere with fundamental rights of individuals, for example when States would engage in extensive cyber monitoring.[228] It must be noted that per *Bosnian Genocide,* the due diligence obligation can only authorise acts compatible with international law.[229] Second, it would make less cyber-capable States more vulnerable to international reaction

---

[221] ICJ, Pulp Mills on the River Uruguay (Argentine v. Uruguay), *I.C.J. Reports 2010*, paragraph 205: the case concerned a complaint by Argentina against Uruguay about environmental consequences caused by two pulp mills that Uruguay had installed close to the border; K. BANNELIER-CHRISTAKIS, "Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?", *Baltic Yearbook of International Law* 2014, Vol. 14, 23-39, 30.

[222] E. T. JENSEN, "Due Diligence in Cyber Activities" in H. KRIEGER, A. PETERS and L. KREUZER (eds.), *Due Diligence in the International Legal Order*, Oxford, Oxford University Press, 2020, 252-269, 264; K. BANNELIER-CHRISTAKIS, "Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?", *Baltic Yearbook of International Law* 2014, Vol. 14, 23-39, 28-31; E. O. OKWORI, "The Obligation of Due Diligence and Cyber-Attacks: Bridging the Gap Between Universal and Differential Approaches for States", *Ethiopian Yearbook of International Law* 2018, 205-242, 233.

[223] E. T. JENSEN, "Due Diligence in Cyber Activities" in H. KRIEGER, A. PETERS and L. KREUZER (eds.), *Due Diligence in the International Legal Order*, Oxford, Oxford University Press, 2020, 252-269, 265.

[224] C. PATRICK, "Debugging the Tallinn Manual 2.0's Application of Due Diligence Principle to Cyber Operations", *Washington International Law Journal* 2019, Vol. 28(2), 581-604, 601.

[225] R. J. BUCHAN, "Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm" *Journal of Conflict & Security Law* 2016, Vol. 21(3), 429-453, 451.

[226] E. T. JENSEN and S. WATTS, "Cyber Due Diligence", *Oklahoma Law Review* 2021, Vol. 73, 645-710, 697.

[227] E. T. JENSEN, "Due Diligence in Cyber Activities" in H. KRIEGER, A. PETERS and L. KREUZER (eds.) *Due Diligence in the International Legal Order*, Oxford, Oxford University Press, 2020, 252-269, 267.

[228] F. DELERUE, *Cyber Operations and International Law*, Cambridge, Cambridge University Press, 2020, 359.

[229] K. BANNELIER-CHRISTAKIS, "Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?", *Baltic Yearbook of International Law* 2014, Vol. 14, 23-39, 31.

for acts beyond its control. This could constitute a gateway to escalation of the conflict.[230] Third, given the lack of a physical presence, the nature and potential consequences of a cyber activity remain speculative until it manifests.[231] In addition, preventive measures are likely to be futile against ever changing malicious software development.[232] Fourth, the knowledge requirement would be rendered redundant if States bore a continuous preventive duty to assess potential cyberattacks.[233]

c. Conclusion

61. While it could be seen as a solution to State responsibility in cyberspace, the issue of due diligence opens a whole array of questions, such as the exact thresholds of knowledge, the capacities of a State, or the extent of the duties. This author agrees that a preventive understanding of the due diligence obligation poses a disproportionate threat to fundamental rights of individuals. And even if a slippery slope of justifying mass surveillance[234] may be too far-fetched, a preventive monitoring duty can also be called into question for two further reasons. First, as explained above, the instantaneous and ever-changing nature of cyber threats may undermine the effectiveness of preventive monitoring. Second, it is technically demanding and thus may exceed the reasonable and feasible character of the due diligence duties.[235] Furthermore, this author agrees that the Tallinn Manual's understanding of due diligence is not *lex lata* and, moreover, not useful because of its complexity.[236]

62. It seems as if the fascination with furthering due diligence duties stems from concern about the inaptitude of the attribution rules. This focus is counterproductive and risks stretching due diligence beyond its limits, rendering it unacceptable to States while not providing much added value. Therefore, a more traditional 'lightweight' due diligence obligation, which is triggered more easily but which entails less severe duties for the State, may perhaps be more effective. It also seems to be more in line with *opinio iuris* of States.[237] After all, it should be recalled that States refrained from a binding formulation of the

---

[230] E. T. JENSEN and S. WATTS, "Cyber Due Diligence", *Oklahoma Law Review* 2021, Vol. 73, 645-710, 694-695, 701; E. T. JENSEN and S. WATTS, "A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer?", *Texas Law Review* 2017, Vol. 95, 1555-1577, 1573.
[231] I. Y. LIU, "The Due Diligence Doctrine Under Tallinn Manual 2.0", *Computer Law & Security Review* 2017, Vol. 33(3), 390-395, 395.
[232] I. Y. LIU, "The Due Diligence Doctrine Under Tallinn Manual 2.0", *Computer Law & Security Review* 2017, Vol. 33(3), 390-395, 395.
[233] I. Y. LIU, "The Due Diligence Doctrine Under Tallinn Manual 2.0", *Computer Law & Security Review* 2017, Vol. 33(3), 390-395, 395.
[234] F. DELERUE, *Cyber Operations and International Law*, Cambridge, Cambridge University Press, 2020, 360.
[235] F. DELERUE, *Cyber Operations and International Law*, Cambridge, Cambridge University Press, 2020, 362.
[236] F. DELERUE, *Cyber Operations and International Law*, Cambridge, Cambridge University Press, 2020, 371.
[237] P. ROGUSKI, "Application of International Law to Cyber Operations: A Comparative Analysis of State's Views", The Hague Program for Cyber Norms Policy Brief, 2020, 48 p., 11-12.

principle within both the UN GGE and OEWG.[238] A recent event may be seen as an example of such a lightweight cyber due diligence obligation in action: on the request of the United States, Russia dismantled a hacking group operating on its territory that was responsible for the attack on the U.S. Colonial Pipeline and prosecuted the members.[239] Russia was made aware that its territory was being used for acts infringing upon the rights of the United States and took reasonable and feasible measures in order to end the threat. A 'lightweight' due diligence obligation does not require more preventive action than the *Bosnian Genocide* standard of a reasonable State in relation to an operation that is underway.[240] This is in line with the classic knowledge requirement. Nevertheless, it presupposes that States undertake their international obligations in good faith and take appropriate steps towards capacity-building (e.g. the establishment of a legal framework and enforcement regime).[241] If there is a degree of prevention, it can only be in a remedial fashion: given the instantaneous nature of cyber operations, a State's due diligence obligation extends up until the moment the particular threat has been neutralised.[242]

2.2.4. Use of force, non-intervention and sovereignty

63. Because the object of this thesis is to analyse the obligations of States in a cyber conflict, the notions of sovereignty, non-intervention and use of force must be approached from this perspective. As explained above, a State can only be held responsible for an internationally wrongful act.[243] Indeed, even if inter-State cyber operations are "*detrimental, objectionable or otherwise unfriendly*", States do not incur responsibility insofar the operations do not breach an international obligation.[244] As such, an offensive cyber operation may have no international legal consequences if it is not understood as an internationally wrongful act.[245] Because of the focus of this thesis is on State obligations, the notion of an 'armed attack' is not separately studied because it serves to justify the right to self-defence

---

[238] United Nationals General Assembly, "Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communication technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266", *A/76/136*, 13 July 2021, 141.

[239] "Russia takes down REvil hacking group at U.S. request – FSB", 14 January 2022, available at: https://www.reuters.com/technology/russia-arrests-dismantles-revil-hacking-group-us-request-report-2022-01-14/.

[240] ICJ, *Bosnian Genocide*, paragraph 431; Tallinn Manual 2.0, 43.

[241] T. DIAS and A. COCO, *Cyber due diligence in international law*, Oxford Institute for Ethics, Law and Armed Conflict, 138-139, available at: https://elac.web.ox.ac.uk/files/finalreport-bsg-elac-cyberduediligenceininternationallawpdf; R. KOLB, "Reflections on Due Diligence Duties and Cyberspace", *German Yearbook of International Law* 2015, Vol. 58, 113-128, 123.

[242] F. DELERUE, *Cyber Operations and International Law*, Cambridge, Cambridge University Press, 2020, 374; M. SCHMITT, "In Defense of Due Diligence in Cyberspace", *The Yale Law Journal Forum* 2015, Vol. 125, 68-81, 75.

[243] ILC, ARSIWA, 32 (Article 1 and its commentary) and 34 (Article 2 and its commentary).

[244] ILC, ARSIWA, 31 (paragraph 4(c) of the general commentary); Tallinn Manual 2.0, 85-86.

[245] W. BANKS, "Who Did It? Attribution of Cyber Intrusions and the Jus In Bello" in R. T. P. ALCALA and E. T. JENSEN (eds.), *The Impact of Emerging Technologies on the Law of Armed Conflict*, Oxford, Oxford University Press, 2019, 235-272, 250.

under the Charter of the United Nations.[246] Evidently, States are *a fortiori* prohibited from committing unlawful armed attacks by cyber means.

It is clear that an in-depth analysis of each concept would lead too far. It does not help that the exact content of each notion is disputed already in their non-cyber application. Rather, these notions are used to understand which acts States must refrain from, either themselves or through non-State actors. This section is also necessary for a good comprehension of the case study (*infra*, p. 79).

a. Use of force

64. The Charter of the United Nations famously prohibits both the use of force and the threat of force in its article 2(4).[247] The concepts of 'use of force' and 'threat of force' are not defined by the Charter and have been given meaning by subsequent caselaw and State practice.[248] The notions are still subject to debate in doctrine.[249] At the same time, doctrine does not exclude the possibility of a cyber operation qualifying as a use of force.[250] This is in line with the position of the ICJ, which decided in *Nuclear Weapons* that the prohibition applies regardless of the weapons employed.[251] In practice, however, no State has ever publicly qualified a cyber operation as a use of force.[252]

65. Thus, States are prohibited from using force by cyber means. It is generally understood that cyber operations that result, or imminently threat to result, in injury or death of persons, or damage or destruction of objects, qualify as use of force.[253] Basically, the approach is effects-based: cyber operations trigger the use of force threshold if they cause such consequences that would be considered a use of force if they were caused by kinetic means. Therefore, it is unlikely that cyber operations not causing any physical consequences or injuries would ever meet the threshold.[254] This approach is criticised as being too restrictive, for not

---

[246] Article 51 Charter of the United Nations
[247] Article 2(4) Charter of the United Nations.
[248] H. LIN, "Cyber Conflict and International Humanitarian Law", *International Review of the Red Cross* 2012, 886(94), 524.
[249] F. DELERUE, *Cyber Operations and International Law*, Cambridge, Cambridge University Press, 2020, 285.
[250] D. B. SILVER, "Computer Network Attacks as a Use of Force under Article 2(4) of the United Nations Charter", *International Law Studies* 2002, Vol. 76, 73-97, 84; see e.g. on the Stuxnet attack: S. J. SHACKELFORD, S. RUSSEL and A. KUEHN, "Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors", *Chicago Journal of International Law* 2016, Vol. 17(1), 13.
[251] ICJ, Legality of the use by a State of nuclear weapons in armed conflict, Advisory opinion, *I.C.J. Rep.* 1996, paragraph 39.
[252] F. DELERUE, *Cyber Operations and International Law*, Cambridge, Cambridge University Press, 2020, 342.
[253] G. P. CORN and R. TAYLOR, "Symposium on Sovereignty, Cyberspace, and Tallinn Manual 2.0 – Sovereignty in the Age of Cyber" *American Journal Of International Law Unbound*, Vol. 111, 207-212, 208; Tallinn Manual 2.0, 333.
[254] M. ROSCINI, "Cyber operations as a use of force" in N. TSAGOURIAS and R. BUCHAN (eds.), *Research Handbook on International Law and Cyberspace*, Cheltenham, Edward Elgar Publishing, 2015, 233-254, 244; F. DELERUE, *Cyber Operations and International Law*, Cambridge, Cambridge University Press, 2020, 303.

all severe consequences are physical in nature.[255] One proposed alternative is to include "*significant disruption of essential services*" (e.g. health, energy, security, water, transportation and banking).[256] Finally, it must be noted that use of force does not presuppose the involvement of armed forces of a State.[257] Per *Nicaragua*, this means that a State providing a non-State actor with malware and training may have engaged in the use of force if the conduct of the non-State actor amounts to the use of force.[258]

b. Non-intervention

66. The principle of non-intervention is a logical consequence of the sovereignty of the State and prohibits States from intervening directly or indirectly in the internal or external affairs of other States, constituting matters in which a State is permitted to decide freely (*domaine réservé*).[259] The ICJ in *Nicaragua* clarified that intervention is only wrongful when it is coercive, namely when it takes away the free choice of the victim State.[260] The element of coercion is crucial. It can be described as "*the affirmative act designed to deprive another State of its freedom of choice*", or "*the application of pressure*" and need not be physical in nature.[261] The intervention need not necessarily be directed at State infrastructure or involve State activities: it suffices that it is designed to undermine the State's authority over the *domaine réservé.*[262] A State-launched cyber operation against a foreign private company can constitute a prohibited intervention.[263] The United Nations Declaration on Friendly Relations contains some examples, reflective of customary law:[264] "*organising, instigating, assisting, financing, or participating in acts of civil strife or terrorism in another State*".[265]

---

[255] N. MELZER, "Cyberwarfare and International Law", *UNIDIR Resources*, 2011, 14; N. TSAGOURIAS, "Cyber attacks, self-defence and the problem of attribution", *Journal of Conflict & Security Law* 2012, Vol. 17, 233-243.

[256] M. ROSCINI, "Cyber operations as a use of force" in N. TSAGOURIAS and R. BUCHAN (eds.), *Research Handbook on International Law and Cyberspace*, Cheltenham, Edward Elgar Publishing, 2015, 233-254, 253; N. TSAGOURIAS, "Cyberattacks, self-defence and the problem of attribution", *Journal of Conflict & Security Law* 17(2), 229-244, 231; E. T. JENSEN, "Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defence" *Standford Journal of International Law* 38, 221-229.

[257] Tallinn Manual 2.0, 331-332.

[258] ICJ, Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Judgment, *I.C.J. Reports* 1986, paragraph 228.

[259] ICJ, Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Judgment, *I.C.J. Reports* 1986, paragraph 205.

[260] ICJ, Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Judgment, *I.C.J. Reports* 1986, paragraph 205.

[261] Tallinn Manual 2.0, 317; H. MOYNIHAN, *The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention*, Chatham House Research Paper, 2019, 28.

[262] T. D. GILL, "Non-Intervention in the Cyber Context" in K. ZIOLKOWSKI (ed.), *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy*, Tallinn, NATO CCD COE Publication, 2013, 217-238, 222; Tallinn Manual 2.0, 315.

[263] F. DELERUE, *Cyber Operations and International Law*, Cambridge, Cambridge University Press, 2020, 240.

[264] ICJ, Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), Judgment, *I.C.J. Reports* 2005, paragraph 162.

[265] Resolution of the UN General Assembly, Declaration on Principles of International law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations (24 Oct 1970). *UN.Doc.* A/RES/25/2625, Principle 1.

Certainly, cyber operations may constitute a prohibited intervention.[266] This could be the case for cyber operations not causing physical effects or injury, and thus not resulting in the use of force, but which satisfy the coercion element.[267] This could be the case for sabotage.[268] Finally, a cyber operation targeting critical State infrastructure (e.g. essential medical facilities, water, energy, security) is likely to amount to a prohibited intervention.[269]

c. Sovereignty

67. Cyber operations not amounting to a prohibited intervention, or a use of force could still be unlawful violations of sovereignty.[270] Sovereignty in cyberspace is perhaps the least settled.[271] A major debate revolves around sovereignty-as-a-principle or sovereignty-as-a-rule. Sovereignty-as-a-rule simply means that sovereignty is a rule of international law that may not be breached, while under sovereignty-as-a-principle, (cyber) operations falling below the threshold of a prohibited intervention would not be regulated by international law.[272] A comprehensive research concluded that even the most vocal States on cyber issues disagree on the existence and applicability of an obligation to respect the sovereignty of another State in cyberspace.[273] Despite incomplete consensus, expressed *opinio iuris*, caselaw and doctrine seem to favour the sovereignty-as-a-rule approach.[274] This means that a violation of sovereignty occurs whenever, without consent, a State exercises its authority in another State's territory in an

---

[266] W. BANKS, "Who Did It? Attribution of Cyber Intrusions and the Jus In Bello" in R. T. P. ALCALA and E. T. JENSEN (eds.), *The Impact of Emerging Technologies on the Law of Armed Conflict*, 2019, Oxford, Oxford University Press, 235-272, 246.

[267] Tallinn Manual 2.0, 318.

[268] T. D. GILL, "Non-Intervention in the Cyber Context" in K. ZIOLKOWSKI (ed.), *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy*, Tallinn, NATO CCD COE Publication, 2013, 217-238, 234.

[269] F. DELERUE, *Cyber Operations and International Law*, Cambridge, Cambridge University Press, 2020, 240; H. MOYNIHAN, *The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention*, Chatham House Research Paper, 2019, 44.

[270] H. MOYNIHAN, *The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention*, Chatham House Research Paper, 2019, 11; N. TSAGOURIAS, "Cyberattacks, self-defence and the problem of attribution", *Journal of Conflict & Security Law* 17(2), 229-244, 231.

[271] H. MOYNIHAN, "The Application of International Law to Cyberspace: Sovereignty and Non-Intervention", 13 December 2019, available at: https://www.justsecurity.org/67723/the-application-of-international-law-to-cyberspace-sovereignty-and-non-intervention/.

[272] G. P. CORN and R. TAYLOR, "Symposium on Sovereignty, Cyberspace, and Tallinn Manual 2.0 – Sovereignty in the Age of Cyber" *American Journal Of International Law Unbound*, Vol. 111, 207-212, 211.

[273] P. ROGUSKI, "Application of International Law to Cyber Operations: A Comparative Analysis of State's Views", The Hague Program for Cyber Norms Policy Brief, 2020, 1; Inter-American Juridical Committee, *International Law and State Operations*, 2020, available at: http://www.oas.org/en/sla/iajc/docs/International_Law_and_State_Cyber_Operations_publication.pdf.

[274] United Nationals General Assembly, "Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communication technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266", *A/76/136*, 13 July 2021; L. CHIRCOP, "Territorial Sovereignty in Cyberspace after Tallinn Manual 2.0", *Melbourne Journal of International Law* 2019, Vol. 20(2), 349-377, 356-357.

area over which the territorial State has the exclusive right to exercise its powers independently.[275] According to the Tallinn Manual, all cyber infrastructure situated within a State's territory, both governmental and private, are covered.[276] Importantly, there is no requirement for coercion.

68. A second debate revolves around the threshold for violations of sovereignty. Within sovereignty-as-a-rule, the most conservative approach is to require physical damage or permanent loss of functionality.[277] On the other side of the spectrum, some authors argue that any non-consensual incursion by a State into the territory of another State can qualify as a violation of the sovereignty of the territorial State.[278] This would include acts such as espionage, which in practice is generally not considered to be a violation of sovereignty by States, or at least not publicly denounced as such.[279] The Tallinn Manual takes two different approaches to sovereignty, which are both defended[280] and criticised[281] in doctrine. First, one of territorial integrity. The experts agreed that the remote causation of physical damage or injury constitutes a violation of sovereignty, as well as the remote causation of loss of functionality when the repair or replacement of physical components is necessary.[282] The thresholds are high and not unlike those of use of force (*supra*, p. 39) and an IHL attack (*infra*, p. 50), which does not seem very logical nor useful. The Shamoon attacks, launched by Iran, are regarded as an example of a violation of sovereignty of the victim States because it required the repair or replacement of thousands of oil company's hard drives.[283] The second approach is that of interference with inherent governmental functions of another State, such as social services, taxation, diplomacy, defence and democratic activities. Here, no physical effects are required: interference with data or services necessary for the exercise of governmental functions suffices.[284] That certain such functions would be privatised would be irrelevant.[285] Finally, some authors propose a 'strict inviolability' approach, which covers all cyber interferences above a *de minimis* threshold.[286] A certain harm has to be caused, which means that for example

---

[275] H. MOYNIHAN, *The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention*, Chatham House Research Paper, 2019, 15.
[276] Tallinn Manual 2.0, 18.
[277] L. CHIRCOP, "Territorial Sovereignty in Cyberspace after Tallinn Manual 2.0", *Melbourne Journal of International Law* 2019, Vol. 20(2), 349-377, 360.
[278] N. TSAGOURIAS, "Law, borders and the territorialisation of cyberspace", *Indonesian Journal of International Law*, Vol. 18(4), 523-551, 544; H. MOYNIHAN, *The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention*, Chatham House Research Paper, 2019, 17.
[279] H. MOYNIHAN, *The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention*, Chatham House Research Paper, 2019, 18-20.
[280] M. SCHMITT and L. VIHUL, "Sovereignty in Cyberspace: lex lata vel non?", *American Journal of International Law* 2017, Vol. 111, 213-218.
[281] G. P. CORN and R. TAYLOR, "Symposium on Sovereignty, Cyberspace, and Tallinn Manual 2.0: Sovereignty in the Age of Cyber", *American Journal of International Law* 2017, Vol. 111, 207-212.
[282] Tallinn Manual 2.0, 20-21.
[283] Tallinn Manual 2.0, 21.
[284] Tallinn Manual 2.0, 22.
[285] Tallinn Manual 2.0, 22.
[286] W. H. VON HEINEGG, "Legal Implications of Territorial Sovereignty in Cyberspace" in C. CZOSECK, R. OTTIS and K. ZIOLKOWSKI (eds.), *4th International Conference on Cyber*

cyber espionage would not be covered.[287] The strict inviolability approach seems reasonably strict, seeking a balance between extremes. However, it leaves again open the question of an exact threshold.

69. This author agrees that requiring physical manifestations is inconsistent with the understanding of sovereignty in relation to land, sea and airspace interference.[288] It also leads to illogical results, whereby an operation in which a State agent uses a USB flash drive to introduce malware into cyber infrastructure located in another State would violate sovereignty,[289] regardless of the consequences, while other highly disruptive cyber operations can escape any qualification as an internationally wrongful act. However, while it must be concluded that sovereignty and its implications in cyberspace remain far from settled, it seems that a consequence-based approach is increasingly favoured by States.[290]

d. Conclusion

70. The respective thresholds are not easily translated to situations of cyber conflict. Under *lex lata*, a violation of sovereignty-as-a-rule seems to be predicated on physical manifestations (injury or damage at least requiring the repair or replacement of physical elements) or the interference with quintessential governmental functions. Use of force seems to require an even higher level of physical effects (injury, death, damage or destruction). Therefore, most peacetime cyber operations are likely to constitute a prohibited intervention, provided they are coercive.[291]

Conflict, NATO Cooperative Cyber Defence Centre of Excellence, 2012, 11; L. CHIRCOP, "Territorial Sovereignty in Cyberspace after Tallinn Manual 2.0", *Melbourne Journal of International Law* 2019, Vol. 20(2), 349-377, 362.

[287] L. CHIRCOP, "Territorial Sovereignty in Cyberspace after Tallinn Manual 2.0", *Melbourne Journal of International Law* 2019, Vol. 20(2), 349-377, 362.

[288] L. CHIRCOP, "Territorial Sovereignty in Cyberspace after Tallinn Manual 2.0", *Melbourne Journal of International Law* 2019, Vol. 20(2), 349-377, 361.

[289] Tallinn Manual 2.0, 19.

[290] Tallinn Manual 2.0, 26.

[291] F. DELERUE, *Cyber Operations and International Law*, Cambridge, Cambridge University Press, 2020, 44.

The challenge is to provide a legal qualification and solution for those cyber operations that cause considerably harmful consequences without causing (some degree of) physical damage. A physical manifestation is not representative of the harm caused. Evidently, there needs to be some threshold to exclude operations merely resulting in inconvenience. However, the Tallinn Manual approach requiring the repair or replacement of physical components is again concerned with the presence of physical elements that have no necessary correlation whatsoever with the actual harmful consequences of the cyber operation. Perhaps a consequence-based approach inspired by the "(*significant*) *disruption of essential services*" proposal could be useful.[292] Another concrete proposal could be the establishment of cyber safe zones in Treaty form.[293] This could circumvent the qualification problem and prohibit State parties from damaging, (significantly) disrupting, and rendering useless critical national infrastructure agreed-upon, outside the context of an armed conflict.

2.3. INTERNATIONAL CYBER ARMED CONFLICTS

2.3.1. Introduction

a. The law of armed conflict

71. The law of armed conflict (international humanitarian law or IHL) seeks both to preserve a sense of humanity in times of war and to mitigate the harmful effects of an armed conflict.[294] The laws are mainly vested in customary international law and the 1949 Geneva Conventions and their Additional Protocols. IHL is a specialised legal regime that only applies to situations of armed conflict, either international or non-international. The existence of an armed conflict is factually determined.[295] A conflict might even be qualified as an armed conflict even if the actors involved do not consider it as such.[296] However, the qualification of cyber armed conflicts will mostly depend on future State practice.[297]

---

[292] M. ROSCINI, "Cyber operations as a use of force" in N. TSAGOURIAS and R. BUCHAN (eds.), *Research Handbook on International Law and Cyberspace*, Cheltenham, Edward Elgar Publishing, 2015, 233-254, 253; N. TSAGOURIAS, "Cyberattacks, self-defence and the problem of attribution", *Journal of Conflict & Security Law* 17(2), 229-244, 231; E. T. JENSEN, "Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defence" *Standford Journal of International Law* 38, 221-229.

[293] See for example the informal attempts between the United States and Russia: https://www.reuters.com/technology/biden-tells-putin-certain-cyber-attacks-should-be-off-limits-2021-06-16/.

[294] B. SAUL and D. AKANDE (eds.), *The Oxford Guide to International Humanitarian Law*, Oxford, Oxford University Press, 2020, 1.

[295] H. H. DINNISS, *Cyber Warfare and the Laws of War*, Cambridge, Cambridge University Press, 2012, 117.

[296] C. GREENWOOD, "Scope of Application of Humanitarian Law" in D. FLECK (ed.), *The Handbook of International Humanitarian Law*, New York, Oxford University Press, 2008, 45.

[297] C. DROEGE, "Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians", *International Review of the Red Cross* 2012, Vol. 94(886), 549.

b. Applicability

72. Cyberspace has been described as the fifth domain or dimension of armed conflict, in addition to land, sea, air and outer space.[298] The United States have recognised cyberspace as an operational domain since 2011.[299] In 2016, NATO did the same.[300] Despite the recognition of operational importance, States cannot seem to agree on the actual application of IHL in cyberspace, as is evidenced by the diffidence of States in the most recent GGE and OEWG reports.[301] If States and other actors are unable to agree on common rules, then IHL, which relies heavily on *opinio iuris* and common practice, may be in danger of losing its ability to foster compliance.[302]

73. The problematic question is whether IHL applies in cyberspace, and if so, how. There may be two, seemingly opposing, views on answering this first question. One lies in the reasoning of the ICJ in *Nuclear Weapons*, stating that the existing law of armed conflict applies to any use of force, regardless of the weapons employed.[303] The other one lies in the famous *Lotus* principle put forward by the predecessor of the ICJ, the Permanent Court of International Justice, namely that acts not forbidden in international law are generally permitted.[304] The first view is supported by the ICRC, and seemingly by an increasing number of States and international organisations.[305] For example, in the first substantive session of the 2021-2025 OEWG, the majority of participating States agreed that IHL is applicable in cyberspace.[306] In practice, however, no State has officially claimed the application of IHL in relation to cyber operations[307], but this might be explained by States' "*policy of ambiguity*

---

[298] J. R. WILSON, "Cyber Warfare Ushers in 5th Dimension of Human Conflict, *Military & Aerospace Electronics* 2014, 25(12), 8-15.

[299] UNITED STATES DEPARTMENT OF DEFENCE, *Department of Defence Strategy for Operating in Cyberspace*, 2011, 5, available at: https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.

[300] NATO Secretary General Stoltenberg Press Conference following the North Atlantic Council meeting at the level of NATO defence ministers, 14 June 2016, https://www.nato.int/cps/en/natohq/opinions_132349.htm?selectedLocale=en, consulted on 5 May 2021.

[301] Report A/AC.290/20121/CRP.2 of the Open-ended working group on developments in the field of information and telecommunications in the context of international security, 10 March 202; Report A/76/135 of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, 14 July 2021.

[302] D. DJUKIC and N. PONS (eds.), *The Companion to International Humanitarian Law*, Leiden, Brill Nijhoff, 2018, p. xxiv.

[303] ICJ, Legality of the use by a State of nuclear weapons in armed conflict, Advisory opinion, *I.C.J. Rep.* 1996, para. 39 and 86.

[304] Permanent Court of International Justice, The Case of the S.S. Lotus (France v. Turkey), *PCIJ Series A no.10*, 1927, 18-19.

[305] ICRC Position Paper on International Humanitarian Law and Cyber Operations during Armed Conflicts, 2019, 4.

[306] Geneva Internet Platform Digwatch, https://dig.watch/events/un-oewg-2021-2025-1st-substantive-session/international-law.

[307] L. CHIRCOP, "A Due Diligence Standard of Attribution in Cyberspace", *International & Comparative Law Quarterly* 2018, Vol. 67, 643-668, 653.

and silence".[308] The Tallinn Manual decided unanimously that IHL applies to situations of cyber warfare.[309] Nevertheless, the Tallinn Manual is filled with examples in which the experts could not achieve consensus on the precise interpretation with respect to cyber operations.[310]

c. The Martens Clause

74. The Martens Clause states that in the absence of legal regulation in treaty-based or customary laws of armed conflict, the principles of humanity and the dictates of the public conscience must govern the conduct on the battlefield.[311] What this means exactly has been the subject of debate. Interpreted restrictively, it highlights that customary international law continues to apply after the adoption of a new treaty norm, but a broader interpretation would mean that not only custom and treaties control the conduct of an armed conflict, but also 'the principles of humanity and the dictates of public conscience'.[312] In any case, the logic of the Martens clause is to avoid a legal vacuum and corresponding loss of protection.[313] As such, the ICJ recognises the Martens clause as an effective means of addressing the evolution of military technology, stating that it has to be observed by all States because it constitutes an intransgressible principle of international customary law.[314] Some consider it to be a *sui generis* source of international law.[315] Both the ICRC and the Tallinn Manual adopt a similar stance to ICJ.[316] According to some, the inclusion of responsible State behaviour in the OEWG and UN GGE final reports could also be seen as an application

---

[308] D. EFRONY and Y. SHANY, "A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice", *The American Journal of International Law*, Vol. 112(4), 583-657; H. MOYNIHAN, *The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention*, Chatham House Research Paper, 2019, 10.

[309] *Tallinn Manual 1.0, 5*; *Tallinn Manual 2.0,* Rule 80.

[310] M. N. SCHMITT and L. VIHUL, "The Nature of International Law Cyber Norms" in A. M. OSULA and H. ROIGAS (eds.), *International Cyber Norms – Legal, Policy & Industry Perspectives*, Tallinn, NATO Cooperative Cyber Defence Centre of Excellence, 2016, 34.

[311] Art. 1(2) Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) of 8 June 1977, *United Nations Treaty Service*, 1125, 3; Paragraph 9 of the Preamble to the Convention (II) with Respect to the Laws and Customs of War on Land of 29 July 1899; Paragraph 8 of the Preamble to the Convention (IV) Respecting the Laws and Customs of War on Land of 18 October 1907.

[312] R. TICEHURST, "The Martens Clause and the Laws of Armed Conflict", *International Review of the Red Cross* 1997, no. 317, available at: https://www.icrc.org/en/doc/resources/documents/article/other/57jnhy.htm; D. DJUKIC and N. PONS (eds.), *The Companion to International Humanitarian Law*, Leiden, Brill Nijhoff, 2018, 471-473; ICRC, Position Paper, 4.

[313] Report A/49/10 of the International Law Commission on the Work of its Forty-sixth Session, 2 May - 22 July 1994.

[314] ICJ, Legality of the use by a State of nuclear weapons in armed conflict, Advisory opinion, *I.C.J. Rep.* 1996, para. 257.

[315] T. SMITH, "Challenges in identifying binding Martens Clause rules from the dictates of the public conscience to protect the environment in non-international armed conflict", *Transnational Legal Theory* 2019, Vol. 10(2), 184.

[316] Tallinn Manual 2.0, 377-378.

of a Martens clause logic.[317] Generally, the Martens Clause is used as an argument that there is no legal vacuum for armed conflicts in cyberspace.[318]

75. The Martens Clause, when viewed as elevating the principles of humanity and the dictates of the public conscience to the level of independent sources of international law, could be very relevant in the context of cyber armed conflicts, where important rules remain disputed.[319] However, the Martens Clause is notable for its "*vagueness and its paucity of application in practice*".[320] In any case, it is evidence of the dynamic approach that is part of IHL and its aid to judicial interpretation and norm-creation.[321] It supports the claim that existing IHL applies to cyber armed conflicts.

2.3.2. International armed conflict

76. As explained earlier, non-international armed conflicts are excluded from the scope of this research. An international armed conflict arises whenever there is resort to armed force between at least two State actors.[322] First, State involvement and thus attribution is an essential prerequisite.[323] State involvement is not measured by the *Nicaragua* threshold of effective control (*supra*, p. 21) for the purpose of conflict qualification.[324] Rather, it is generally accepted that the threshold is one of 'overall control', adopted by the ICTY in *Tadic* and confirmed by the ICJ for the purpose of conflict qualification in *Bosnian*

---

[317] M. KAIJURAND, "United Nations Group of Governmental Experts: The Estonian Perspective" in A. M. OSULA and H. ROIGAS (eds.), *International Cyber Norms – Legal, Policy & Industry Perspectives*, Tallinn, NATO Cooperative Cyber Defence Centre of Excellence, 2016, 125; Report A/AC.290/20121/CRP.2 of the Open-ended working group on developments in the field of information and telecommunications in the context of international security, 10 March 2021, 4-6, available at: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.

[318] R. GEISS and H. LAHMANN, "Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space", *Israel Law Review* 2012, Vol. 45(3), 381-399, 382.

[319] R. TICEHURST, "The Martens Clause and the Laws of Armed Conflict", *International Review of the Red Cross 1997*, no. 317, available at: https://www.icrc.org/en/doc/resources/documents/article/other/57jnhy.htm; D. DJUKIC and N. PONS (eds.), *The Companion to International Humanitarian Law*, Leiden, Brill Nijhoff, 2018, 700; T. D. EVANS, "At war with the robots: autonomous weapon systems and the Martens clause", *Hofstra Law Review* 2013, Vol. 41(3), 697-734; M. SCHMITT, "Wired warfare 3.0: Protecting the civilian population during cyber operations", *International Review of the Red Cross* 2019, Vol. 101(1), 333-355, 344.

[320] M. SCHMITT, "Wired warfare 3.0: Protecting the civilian population during cyber operations", *International Review of the Red Cross* 2019, Vol. 101(1), 333-355, 354.

[321] K. BANNELIER-CHRISTAKIS; "Is the principle of distinction still relevant in cyberwarfare?" in N. TSAGOURIAS and R. BUCHAN (eds.), *Research Handbook on International Law and Cyberspace*, Cheltenham, Edward Elgar Publishing, 2015, 343-365, 356; M. SALTER, "Reinterpreting Competing Interpretations of the Scope and Potential of the Martens Clause", *Journal of Conflict and Security Law* 2012, Vol. 17(3), 403-437, 437.

[322] Common Article 2 of the Geneva Conventions of 1949; ICTY, *Prosecutor v Tadic* (Appeals Chamber Decision on the defence motion for interlocutory appeal on jurisdiction), 2 October 1995, paragraph 70.

[323] C. DROEGE, "Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians", *International Review of the Red Cross* 2012, Vol. 94(886), 541.

[324] M. N. SCHMITT and L. VIHUL, "Proxy Wars in Cyberspace: The Evolving International Law of Attribution", *Fletcher Security Review* 2014, Vol. 1(2), 71.

Genocide.[325] Concretely, this means that the threshold is a lower one: there is no need to prove that each operation was carried out on the instructions of the State, or under its effective control.[326] Nevertheless, even in times of armed conflict, States bear responsibility for conduct of non-State actors under the standard rules of attribution (*supra*, p. 19).[327] To that effect, see the Montreux Document, which is concerned with Private Military and Security Companies (PMSCs) in situations of armed conflict.[328] Others argue that once an armed conflict exists, it is lawful to presume that incoming operations are the responsibility of the opponent.[329] Specifically under IHL, Common Article 1 to the Geneva Conventions imposes on States the duty to ensure the respect of IHL in all circumstances, including by actors not officially member of the armed forces.[330]

77. Second, there must be resort to armed force. It is important to flag that the notions of the *ius contra bellum* and the *ius in bello* do not implicate one another, meaning that a use force does not necessarily qualify as an armed force and vice versa.[331] In the absence of a treaty definition of what constitutes 'armed force' under IHL, one must look to caselaw.[332] Controversy exists on the threshold of requisite violence.[333] Under *lex lata*, it remains uncertain whether cyber operations alone can qualify as 'armed force' and trigger the application of IHL. If not, an armed conflict can only arise when there are parallel physical offensive operations between the two States. If cyber operations are connected to such a physical armed conflict, qualification and application may become easier.[334] Arguably, this is a strange situation, whereby the application of the legal framework no longer depends on the ratio of IHL, but rather on the means and methods of warfare exploited. This while humanitarian risks to cyber operations

---

[325] International Yugoslavia Tribunal, *Prosecutor v Tadic*, Decision on Jurisdiction, Case no. IT-94-1-AR 72, 2 October 1995 (the case concerned the individual prosecution of Mr. Tadic for war crimes committed at a concentration camp); ICJ, *Bosnian Genocide*, paragraph 404.

[326] ICJ, *Bosnian Genocide*, paragraph 402.

[327] W. BANKS, "Who Did It? Attribution of Cyber Intrusions and the Jus In Bello" in R. T. P. ALCALA and E. T. JENSEN (eds.), *The Impact of Emerging Technologies on the Law of Armed Conflict*, 2019, Oxford, Oxford University Press, 235-272, 260.

[328] International Committee of the Red Cross and Federal Department of Foreign Affairs of Switzerland, The Montreux Document on pertinent international legal obligations and good practices for States related to operations of private military and security companies during armed conflict, 2009, 12, available at: https://www.icrc.org/en/doc/assets/files/other/icrc_002_0996.pdf

[329] W. BANKS, "Who Did It? Attribution of Cyber Intrusions and the Jus In Bello" in R. T. P. ALCALA and E. T. JENSEN (eds.), The Impact of Emerging Technologies on the Law of Armed Conflict, 2019, Oxford, Oxford University Press, 2019, 235-272, 259.

[330] L. DOSWALD-BECK, "Private military companies under international humanitarian law" in S. CHESTERMAN and C. LEHNARDT (eds.), From Mercenaries to Market: The Rise and Regulation of Private Military Companies, Oxford, Oxford University Press, 115-138, 132.

[331] C. DROEGE, "Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians", International Review of the Red Cross 2012, Vol. 94(886), 545.

[332] C. DROEGE, "Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians", International Review of the Red Cross 2012, Vol. 94(886), 546.

[333] Tallinn Manual 2.0, 383.

[334] E. DIAMOND, "Applying International Humanitarian Law to Cyber Warfare" in P. S. BARUCH and A. KURZ (eds.), *Law and National Security: Selected Issues*, Institute for National Security Studies, 2014, 71; T. D. GILL, "International humanitarian law applied to cyber-warfare: precautions, proportionality and the notion of 'attack' under the humanitarian law of armed conflict" in N. TSAGOURIAS and R. BUCHAN (eds.), *Research Handbook on International Law and Cyberspace*, Cheltenham, Edward Elgar Publishing, 2015, 366-379, 370.

are clearly established. The ICJ's confirmation in *Nuclear Weapons* that the purposes of international humanitarian law are not bound by the means or methods of warfare used can also be highlighted.[335]

78. The Tallinn Manual pleaded to keep the threshold for a cyber armed conflict relatively low, as it is for traditional kinetic armed conflicts,[336] but no definite threshold was decided.[337] The International Law Association concluded that an armed conflict requires "*fighting of some intensity*".[338] The same study found that State practice supports distinguishing armed conflicts from *inter alia* 'incidents' and 'border clashes'.[339] So, despite a relatively low threshold, isolated incidents are almost never considered triggering IHL.[340] Nevertheless, there is no requirement of duration of the conflict for IHL to apply.[341] This means that the instantaneous nature of cyber operations legally does not prevent the application of IHL.

2.3.3. Conduct of hostilities

a. Are cyber operations attacks?

79. Instances of cybercrime and offensive cyber operations are on the rise. News articles often headline with notions such as 'cyberattack' or 'cyberwarfare'. For this reason, it is important to insist on the correct legal terminology under IHL. Indeed, even if IHL is triggered in a conflict where cyber operations are being used, cyber operations are not automatically regulated by the IHL rules on the conduct of hostilities. The Additional Protocol I to the 1949 Geneva Conventions (AP I) contains the most important IHL principles on the conduct of hostilities, such as the principles of distinction, proportionality and precaution.[342] The wording of these principles in AP I seem to require an 'attack' for their application. For example, the Tallinn Manual and the U.S. Law of War

---

[335] ICJ, Legality of the use by a State of nuclear weapons in armed conflict, Advisory opinion, *I.C.J. Rep.* 1996.

[336] International Law Association, *Final Report on the Meaning of Armed Conflict in International Law*, 2010, available at: http://www.rulac.org/assets/downloads/ILA_report_armed_conflict_2010.pdf; L. ARIMATSU, "Classifying cyber warfare" in N. TSAGOURIAS and R. BUCHAN (eds.), *Research Handbook on International Law and Cyberspace*, Cheltenham, Edward Elgar Publishing, 2015, 326-342, 330.

[337] Tallinn Manual 2.0, 383-384.

[338] International Law Association, *Final Report on the Meaning of Armed Conflict in International Law*, 2010, 32, available at: http://www.rulac.org/assets/downloads/ILA_report_armed_conflict_2010.pdf

[339] International Law Association, *Final Report on the Meaning of Armed Conflict in International Law*, 2010, 28, available at: http://www.rulac.org/assets/downloads/ILA_report_armed_conflict_2010.pdf

[340] S. VERHOEVEN, "International and Non-International Armed Conflicts" in J. WOUTERS, P. DE MAN and N. VERLINDEN (eds.), *Armed Conflicts and the Law*, Mortsel, Intersentia, 2016, 151-186, 158.

[341] S. VERHOEVEN, "International and Non-International Armed Conflicts" in J. WOUTERS, P. DE MAN and N. VERLINDEN (eds.), *Armed Conflict and the Law*, Mortsel, Intersentia, 2016, 151-185, 158.

[342] Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the protection of victims of international armed conflicts, 8 June 1977 (hereinafter: AP I), articles 49-58.

Manual take this approach, excluding operations that do not reach the threshold of an 'attack'.[343] This is not without critique.[344]

80. The Tallinn Manual defines cyberattacks for this purpose as cyber operations that are reasonably expected to cause injury or death to persons or damage or destruction to objects.[345] For this definition, the Tallinn Manual draws on article 49(1) AP I, which defines an attack as an "*act of violence*" against the adversary. It is clear that the violent nature is crucial to distinguish between cyber operations that qualify as attacks and those that do not. For this reason, psychological cyber operations, mere attacks on the morale and cyber espionage are not attacks.[346] The same is true for non-destructive cyber exploitations seeking to collect information.[347] It is also clear, however, that violence need not be kinetic.[348] A majority of experts in the Tallinn Manual agreed that that loss of functionality also qualifies as damage, but there was no agreement on the exact extent of such loss.[349] In any case, a cyber operation destroying data is not considered an attack insofar as it does not affect any functionality.[350] The experts also reasoned that a cyber operation does not need to result in the intended destructive effect to qualify as an attack, and that a failed or prevented attack is still an attack.[351]

81. On the other hand, the ICRC argues that any operation intended to disable an object, such as a computer or a computer network, qualifies as an attack for the purpose of IHL, regardless of the means used.[352] The focus on intent may seem controversial but the approach seems influenced by the wording of article 52(2) AP I: "*Attacks shall be limited strictly to military objectives. In so far as*

---

[343] Tallinn Manual 2.0, 415; United States Department of Defense, *Law of War Manual*, June 2015 (updated December 2016), 1020, paragraph 16.5.1, available at: https://dod.defense.gov/Portals/1/Documents/pubs/DoD%20Law%20of%20War%20Manual%20-%20June%202015%20Updated%20Dec%202016.pdf?ver=2016-12-13-172036-190.

[344] C. DROEGE, "Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians", *International Review of the Red Cross* 2012, Vol. 94(886), 554; M. N. SCHMITT, "Cyber Operations and the Ius in Bello: Key Issues", *International Law Studies* 2011, Vol. 87, 89-110, 91-92; N. MELZER, *Cyberwarfare and International Law*, UNIDIR Resources Paper, 2011, 24, available at: https://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf.

[345] Tallin Manual 2.0, 415.

[346] Tallinn Manual 2.0, 415; C. DROEGE, "Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians", *International Review of the Red Cross* 2012, Vol. 94(886), 559; N. LUBELL, "Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply?", *International Law Studies* 2013, Vol. 89, 252-275, 273.

[347] M. ROSCINI, "Cyber operations as a use of force" in N. TSAGOURIAS and R. BUCHAN (eds.), *Research Handbook on International Law and Cyberspace*, Cheltenham, Edward Elgar Publishing, 2015, 233-254, 240.

[348] Military operations using biological and chemical weapons are considered attacks because of the consequences they cause: see K. DÖRMANN, "Applicability of the Additional Protocols to Computer Network Attacks", *CICR Resources*, 19 November 2004, 4, available at: https://www.icrc.org/en/doc/assets/files/other/applicabilityofihltocna.pdf.

[349] Tallinn Manual 2.0, 417.

[350] W. BANKS, "Who Did It? Attribution of Cyber Intrusions and the Jus In Bello" in R. T. P. ALCALA and E. T. JENSEN (eds.), *The Impact of Emerging Technologies on the Law of Armed Conflict*, 2019, Oxford, Oxford University Press, 2019, 235-272, 257.

[351] Tallinn Manual 2.0, 419.

[352] ICRC Position Paper, 7-8.

objects are concerned, military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralisation, in the circumstances ruling at the time, offers a definite military of advantage".[353] Likewise, several authors point out that the term 'neutralisation', next to 'destruction' and 'capture', in the article 52(2) AP I definition implies that non-kinetic operations can qualify as attacks.[354] In addition, the ICRC argues that harm also includes foreseeable direct and indirect effects of the attack, which would for example include the death of patients caused by a cyber operation launched against a hospital's electricity network.[355] Along these lines, one author proposes that the destruction of or damage to medical data or operational data of a public utility is *always* reasonably expected to cause physical injury or damage and therefore always constitutes an attack.[356]

82. In general, operations that cause inconvenience or irritation might be severe, but they do not qualify as attacks, even if the effects on civilians are significant.[357] Certainly, cyber operations more often cause cyber harm, for example by manipulating or destroying data, than physical damage or injury.[358] Therefore, the threshold rules out the majority of cyber operations from being covered by IHL principles, despite them having the capacity to cause serious adverse consequences for the civilian population.[359] This understanding also seems to mean that under IHL, States can lawfully target civilians and civilian infrastructure within another State as long as there is no physical damage.[360] For these reasons, it can be called into question whether physical damage is the only test for the threshold.[361]

---

[353] Art. 52(2) AP I.

[354] K. DÖRMANN, "Applicability of the Additional Protocols to Computer Network Attacks", *CICR Resources*, 19 November 2014, 4, available at: https://www.icrc.org/en/doc/assets/files/other/applicabilityofihltocna.pdf; C. DROEGE, "Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians", *International Review of the Red Cross* 2012, Vol. 94(886), 558.

[355] ICRC Position Paper, 7.

[356] T. D. GILL, "International humanitarian law applied to cyber-warfare: precautions, proportionality and the notion of 'attack' under the humanitarian law of armed conflict" in N. TSAGOURIAS and R. BUCHAN (eds.), *Research Handbook on International Law and Cyberspace*, Cheltenham, Edward Elgar Publishing, 2015, 366-379, 376.

[357] M. N. SCHMITT, "Cyber Operations and the Ius in Bello: Key Issues", *International Law Studies* 2011, Vol. 87, 89-110, 103-104.

[358] W. BANKS, "Who Did It? Attribution of Cyber Intrusions and the Jus In Bello" in R. T. P. ALCALA and E. T. JENSEN (eds.), *The Impact of Emerging Technologies on the Law of Armed Conflict*, Oxford, Oxford University Press, 2019, 235-272, 235.

[359] M. SCHMITT, "Wired warfare 3.0: Protecting the civilian population during cyber operations", *International Review of the Red Cross* 2019, Vol. 101(1), 333-355, 340; P. PASCUCCI, "Distinction and Proportionality in Cyber War: Virtual Problems with a Real Solution", *Minnesota Journal of International Law* 2017, Vol. 26(2), 419-460, 442.

[360] K. BANNELIER-CHRISTAKIS; "Is the principle of distinction still relevant in cyberwarfare?" in N. TSAGOURIAS and R. BUCHAN (eds.), *Research Handbook on International Law and Cyberspace*, Cheltenham, Edward Elgar Publishing, 2015, 343-365, 354.

[361] N. LUBELL, "Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply?", *International Law Studies* 2013, Vol. 89, 252-275, 265.

83. This author agrees that cyber operations can very well qualify as IHL attacks and that the focus should not be on the type of harm but on the level of harm.[362] After all, the criterium seems to be "*violence*".[363] Such a threshold could be referred to as a test of 'kinetic effect equivalency':[364] if a cyber operation disables (neutralises) an object, resulting in a level of harm, which, if it were caused by a kinetic operation, would amount to an attack under IHL, that cyber operation qualifies as an attack.[365] It is clear that cyber operations with the goal of sabotage are not principally to be excluded from qualifying as IHL attacks. However, it would not seem sensible to include all forms of sabotage such as temporal distributed denial-of-service (DDoS)[366] attacks.[367] Therefore, the author is inclined to agree with the majority (respectively minority) position in the Tallinn Manual that operations requiring the replacement of physical components or the reinstalment of the operating system or of particular data amount to IHL attacks.[368] Regardless of the exact threshold, the author also agrees with the line of reasoning that certain cyber operations can *always* reasonably be expected to cause injury to persons or damage to objects if they cause neutralisation of the targeted system.[369] This would be the case for targeting critical infrastructures such as healthcare infrastructure, air traffic control systems and energy plants.

b. Distinction

84. The principle of distinction is set out in articles 48 and 52 AP I. Under the principle of distinction, parties to a conflict must distinguish between military objectives and civilian objects and civilians.[370] According to the ICJ, it is a cardinal principle of IHL with customary status.[371] Interestingly, the basic rule in article 48 AP I obliges States to "direct their *operations* only against military objectives"

---

[362] N. LUBELL, "Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply?", *International Law Studies* 2013, Vol. 89, 252-275, 271.
[363] Article 49(1) AP I.
[364] K. BANNELIER-CHRISTAKIS; "Is the principle of distinction still relevant in cyberwarfare?" in N. TSAGOURIAS and R. BUCHAN (eds.), *Research Handbook on International Law and Cyberspace*, Cheltenham, Edward Elgar Publishing, 2015, 343-365, 348.
[365] It is warned, however, that certain cyber operations may not have a clear kinetic parallel in terms of capabilities and effects, see: United States Department of Defense, *Law of War Manual*, June 2015 (updated December 2016), 1015, paragraph 16.2.2, available at: https://dod.defense.gov/Portals/1/Documents/pubs/DoD%20Law%20of%20War%20Manual%20-%20June%202015%20Updated%20Dec%202016.pdf?ver=2016-12-13-172036-190.
[366] Distributed Denial-of-Service attacks aim to flood the target with traffic, overwhelming it and resulting in temporary loss of functionality (denial of service).
[367] After all, the jamming of radio communications or television broadcasts is not typically considered to be an IHL attack: ICRC, *International humanitarian law and the challenges of contemporary armed conflicts*, Geneva, 2015, 42, available at: https://www.icrc.org/en/document/icrc-report-ihl-and-challenges-contemporary-armed-conflicts.
[368] Tallinn Manual 2.0, 417.
[369] T. D. GILL, "International humanitarian law applied to cyber-warfare: precautions, proportionality and the notion of 'attack' under the humanitarian law of armed conflict" in N. TSAGOURIAS and R. BUCHAN (eds.), *Research Handbook on International Law and Cyberspace*, Cheltenham, Edward Elgar Publishing, 2015, 366-379, 376.
[370] H. LIN, "Cyber Conflict and International Humanitarian Law", *International Review of the Red Cross* 2012, 886(94), 525.
[371] ICJ, Legality of the use by a State of nuclear weapons in armed conflict, Advisory opinion, *I.C.J. Rep.* 1996, paragraph 78-79.

(emphasis added).[372] On the other hand, article 52 AP I, which deals with distinguishing civilian objects and military objectives, only concerns attacks (*supra*, p. 52).

85. Per article 52 AP I, the only permissible targets are military objectives.[373] Under IHL, everything that is not a military objective is a civilian object.[374] Military objectives can be both individuals (combatants or individuals directly participating in hostilities) and objects. Concerning objects, "*military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralisation, in the circumstances ruling at the time, offers a definite military advantage*".[375] There is a three-step test for military objectives. First, one must look at the criteria of nature, location, purpose or use of the object. Second, an object can only be a military objective if it makes an effective contribution to military action. Under the 'use' criterium, this is perhaps the most problematic requirement.[376] It is generally accepted that both war-fighting (objects used for combat) and war-supporting objects (objects making an effective contribution to military action, such as a factory developing the computer guidance system for a weapon) can be military objectives.[377] The United States also include war-sustaining objects (objects making the war and its continuation possible), which certainly in cyberspace could drastically widen the scope of military objectives.[378] The inclusion was rejected in the Tallinn Manual.[379] Likewise, authors argue that for a civilian object to qualify as a military objective, its contribution to military action must be directed towards the actual war-fighting capabilities of a party to the conflict, and not merely contributing to the war-sustaining capability:[380] otherwise, there would be no limits to cyberwarfare.[381] Third, the destruction, capture or neutralisation of the object must offer, in the circumstances ruling at the time, a definite military advantage. This means that the attacker must reasonably conclude that the destruction, capture or neutralisation of the object will result in an actual military advantage.[382]

---

[372] Article 48 AP I.
[373] C. DROEGE, "Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians", *International Review of the Red Cross* 2012, Vol. 94(886), 561.
[374] Article 52(1) AP I.
[375] Article 52(2) AP I.
[376] P. PASCUCCI, "Distinction and Proportionality in Cyber War: Virtual Problems with a Real Solution", *Minnesota Journal of International Law* 2017, Vol. 26(2), 419-460, 433.
[377] P. PASCUCCI, "Distinction and Proportionality in Cyber War: Virtual Problems with a Real Solution", *Minnesota Journal of International Law* 2017, Vol. 26(2), 419-460, 433.
[378] P. PASCUCCI, "Distinction and Proportionality in Cyber War: Virtual Problems with a Real Solution", *Minnesota Journal of International Law* 2017, Vol. 26(2), 419-460, 434.
[379] Tallinn Manual 2.0, 436.
[380] C. DROEGE, "Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians", *International Review of the Red Cross* 2012, Vol. 94(886), 567.
[381] R. GEISS and H. LAHMANN, "Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space", *Israel Law Review* 2012, Vol. 45(3), 381-399, 390; Z. CHANG, "Cyberwarfare and International Humanitarian law", *Creighton International and Comparative Law Journal* 2017, Vol. 9(1), 29-53, 39.
[382] Tallinn Manual 2.0, 443.

86. An important corollary of the principle of distinction is the prohibition of indiscriminate attacks.[383] This supposes that a means of warfare capable of discrimination has been used indiscriminately.[384] Distinction also prohibits States from using weapons that are incapable of distinguishing between civilian and military objectives, or that are uncontrollable or unpredictable.[385] The principle of distinction also is the basis for the principle of proportionality and the principle of precaution. However, all these aspects cannot be mixed up, they will be dealt with separately. Despite its cardinal importance and "*intransgressible*" nature, the principle of distinction is not easily applied in cyberspace.[386] In the next two subsections, the thesis will analyse two of the major challenges. First, the issue of dual-use. Second, the issue of whether civilian data can qualify as civilian objects under IHL.

b.1. Dual-use

87. Dual-use arises whenever an object is used both for civilian and military purposes. Because of the interconnected nature of cyberspace, the issue of dual-use is crucial. Most international cyber infrastructure is in practice dual-use.[387] For example, military communications are often routed over civilian communication facilities.[388] In 2010, 98% of U.S. military data was stored in civilian data centres around the world.[389] Attacking dual-use objectives is not prohibited.[390] The prevailing view is that from the moment an object is used for military action, it becomes a military objective, even if its military use is but marginal.[391] This is because of the so-called 'use' criterium in article 52(2) AP I

---

[383] Art. 51(4)(a)-(c) AP I; ICRC Customary International Humanitarian Law Study, Rule 12, available at: https://ihl-databases.icrc.org/customary-ihl/eng/docindex/v1_rul_rule12.
[384] Tallinn Manual 2.0, 468.
[385] Art. 51(4)(b)-(c) AP I; ICJ, Legality of the use by a State of nuclear weapons in armed conflict, Advisory opinion, *I.C.J. Rep.* 1996, paragraph 78.
[386] ICJ, Nuclear Weapons, paragraphs 78-79.
[387] C. DROEGE, "Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians", *International Review of the Red Cross* 2012, Vol. 94(886), 562.
[388] H. LIN, "Cyber Conflict and International Humanitarian Law", *International Review of the Red Cross* 2012, 886(94), 525.
[389] E. T. JENSEN, "Cyber Warfare and Precautions Against the Effects of Attacks", *Texas Law Review* 2010, Vol. 88, 1533-1569, 1542.
[390] Tallinn Manual 2.0, 445; ICRC Commentary to the 1977 Additional Protocols, paragraph 2023.
[391] Tallinn Manual 2.0, 445; Ministère des Armées, *Droit International Applique aux Operations dans le Cyberespace*, 2019, 15 available at: https://www.justsecurity.org/wp-content/uploads/2019/09/droit-internat-appliqu%C3%A9-aux-op%C3%A9rations-cyberespace-

(*supra*, p. 55).[392] Evidently, this view poses difficulties for cyberspace. From the moment that they are used to transmit military information, major cables, nodes, routers or satellites will qualify as military objectives, despite their important and predominant civilian usage.[393] The Tallinn Manual admits that under a strict application of this approach, the entire internet could become a military objective.[394]

88. For this reason, the ICRC argues that not every use for military purposes renders a civilian object a military objective; it still needs to fulfil the definition of article 52(2) AP I, namely that its destruction, capture or neutralisation must offer a definite military advantage.[395] This is in line with the three-step test for military objectives set out earlier and is much more consistent with protective IHL rules. For example, if there is doubt as to the status of objects, art. 52(3) AP I states that "*in case of doubt whether an object which is normally dedicated to civilian purposes (...) is being used to make an effective contribution to military action, it shall be presumed not to be so used*".[396] There is a rebuttable presumption of civilian nature if the status of such objects is uncertain. However, because of its wording and its doubtful customary status, this rule is seen as being of limited relevance.[397] This is unfortunate, given its potential to protect important civilian cyber infrastructure. There is also article 54(2) AP I, prohibiting operations (not only attacks) that "*render useless objects indispensable for the survival of the civilian population*".[398] Finally, there is article 56 AP I, which prohibits attacks against objects "*containing dangerous forces*", such as dams and nuclear power plants, but only if the attack "*may cause the release of dangerous forces and consequent severe losses among the civilian population*".[399] Some authors argue to widen the scope of this last article to certain cyber infrastructures by analogy.[400]

89. This author concludes that even if, per the prevailing view, any military use of a civilian object renders it a military objective, this does not automatically mean that it can lawfully be targeted. Indeed, it still needs to fulfil the complete article 52(2) AP I definition.[401] For this reason, the three step test is crucial. If an

---

france.pdf; S. VERHOEVEN, "The Protection of Civilians and Civilian Objects Against Hostilities" in J. WOUTERS, P. DE MAN and N. VERLINDEN (eds.), *Armed Conflicts and the Law*, Mortsel, Intersentia, 2016, 259-303, 275.

[392] Article 52(2) AP I; ICRC Commentary to the 1977 Additional Protocols, paragraph 2022.

[393] C. DROEGE, "Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians", *International Review of the Red Cross* 2012, Vol. 94(886), 564.

[394] Tallinn Manual 2.0, 446.

[395] ICRC Position Paper, 7; ICRC Customary International Humanitarian Law Study, Rule 8, available at: https://ihl-databases.icrc.org/customary-ihl/eng/docindex/v1_rul_rule8.

[396] Art. 52(3) AP I.

[397] Tallinn Manual 2.0, 448.

[398] Art. 54(2) AP I.

[399] Art. 56(1) AP I.

[400] R. GEISS and H. LAHMANN, "Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space", *Israel Law Review* 2012, Vol. 45(3), 381-399, 391.

[401] Gary D. Solis creates a cynical but convincing example. In the Vietnam war, bamboo was widely used to make so-called punji stakes to trap and harm U.S. soldiers. Clearly, this did not render bamboo groves military objects and lawful targets, because they do not meet the other criteria in

object is being used by the military (for war-fighting or war-supporting purposes) (1), that use must still make an effective contribution to military action (2), and the total or partial destruction, capture or neutralisation of the object must, in the circumstances ruling at the time, offer a definite military advantage (3). Because these criteria are for the attacking party to assess on a case by case basis, the principles of proportionality and precaution will play an important role (*infra*, p. 61, 63). Finally, this author argues that it is sensible to extend the article 52(3) AP I presumption of civilian nature for objects "*normally dedicated to civilian purposes*" to certain civilian cyber infrastructures such as school networks and networks of civilian hospitals.

b.2. Data protection in cyber armed conflict

90. The issue of data in IHL is much disputed and relates to the question whether data can be considered an 'object' for the purpose of IHL protection. The problem is elevated because data is perhaps an abstract concept. One author makes a useful distinction between content-level data and operational-level data.[402] Content-level data includes personal data, metadata and other contents. Operational-level data refers to program data which gives functionality to hardware, such as software applications. Destruction of operational-level data will result in the (temporary or permanent) loss of functionality of the system.[403] Content-level data probably enjoys a level of protection under international human rights law (*infra*, p. 67).

A majority of the experts of the Tallinn Manual decided that data should not be considered an object because "*data is intangible and therefore neither falls within the ordinary meaning of the term object, nor comports with the explanation offered in the ICRC Additional Protocols 1987 Commentary*".[404] Importantly, the Tallinn Manual does state that whenever an operation against data foreseeably results in the injury or death of individuals or damage or destruction of physical objects, those individuals or objects constitute the object of the operation and the operation therefore qualifies as an attack, despite that the attack was directly targeting data.[405]

91. According to one author, not only is there a historical argument against the adherence to the tangibility requirement, the ICRC Commentary also only used this description of an object to distinguish it from the ordinary meaning of an

---

article 52(2) AP I. See: G. D. SOLIS, *The Law of Armed Conflict: International Humanitarian Law in War*, Cambridge, Cambridge University Press, 2016, 522.

[402] H. H. DINNIS, "The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives, *Israel Law Review* 2015, Vol. 48(1), 39-54, 41.

[403] H. H. DINNIS, "The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives, *Israel Law Review* 2015, Vol. 48(1), 39-54, 42.

[404] Tallinn Manual 2.0, 437; ICRC Commentary of the Additional Protocols, 1987, 634, paragraph 2008, available at: https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Comment.xsp?action=openDocument&documentId=5F27276CE1BBB79DC12563CD00434969.

[405] Tallinn Manual 2.0, 416.

object as a general objective or purpose of a military operation'.[406] The author argues for the qualification of data as objects by using the classic Treaty interpretation methods, as set out in the Vienna Convention on the Law of Treaties.[407] Another author agrees with this analysis, concluding that the law itself does not exclude the possibility of data as objects.[408] To illustrate, while the French language version of AP I does speak of "*biens*", the official French position is that data can form a military objective *and* that civilian content-level data is protected by the principle of distinction.[409]

92. Critics further argue that except for the tangibility issue, data fits perfectly well within the existing IHL rules. One author entertained the option of including data in the non-object category of objectives in article 52(2) AP I.[410] Relying further on article 52(2) AP I, data is indeed susceptible to destruction, capture or neutralisation, and as such fits the description of military objectives.[411] Furthermore, data may provide an effective contribution to military action through its nature, location, purpose or use.[412] If States admit that certain data, such as software allowing for troop communication, is a military objective, they admit that data are objects. Another author heckles an inconsistency by pointing to the lack of a tangibility requirement in IHL when it comes to weapons and means and methods of warfare.[413] Similarly, the Tallinn Manual does consider the possibility of intangible IHL objects when it comes to the protection of cultural objects under article 53 AP I.[414]

93. A minority of the Tallinn Manual experts argued that at least data that is essential to the well-being of the civilian population must be protected as objects under IHL.[415] Comparably, the ICRC argues that certain essential civilian data,

---

[406] ICRC Commentary of the Additional Protocols, 1987, 634, paragraph 2010, available at: https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Comment.xsp?action=openDocument&documentId=5F27276CE1BBB79DC12563CD00434969.

[407] K. MACAK, "Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law", *Israel Law Review* 2015, Vol. 48(1), 55-80, 67-80; Article 31(1) Vienna Convention on the Law of Treaties.

[408] N. LUBELL, "Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply?", *International Law Studies* 2013, Vol. 89, 252-275, 271.

[409] Ministère des Armées, *Droit International Applique aux Operations dans le Cyberespace*, 2019, 14-15, available at: https://www.justsecurity.org/wp-content/uploads/2019/09/droit-internat-appliqu%C3%A9-aux-op%C3%A9rations-cyberespace-france.pdf.

[410] The authors relies on the formulation of article 52(2) AP I "*in so far as objects are concerned*", which is originally meant to distinguish objects as military objectives from persons as military objectives, to argue that data could fit into the latter category of non-objects: K. MACAK, "Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law", *Israel Law Review* 2015, Vol. 48(1), 55-80, 63.

[411] K. MACAK, "Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law", *Israel Law Review* 2015, Vol. 48(1), 55-80, 73.

[412] H. H. DINNISS, "The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives", *Israel Law Review* 2015, Vol. 48(1), 39-54, 54.

[413] H. H. DINNIS, "The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives, *Israel Law Review* 2015, Vol. 48(1), 39-54, 46.

[414] Tallinn Manual 2.0, 535.

[415] Tallinn Manual 2.0, 437.

such as data belonging to medical units, is protected under IHL.[416] The ICRC reasons that "*the replacement of paper files and documents with digital files in the form of data should not decrease the protection that IHL affords to them*".[417] Also, since targeting objects indispensable for the survival of the civilian population is prohibited, data necessary for the functioning of such objects would be protected as well.[418]

94. SCHMITT defends the majority position of the Tallinn Manual to exclude data from qualifying as IHL objects.[419] However, his claim that the destruction of data is similar to psychological operations and thus not covered by AP I finds little support.[420] He also cautioned that the inclusion of data as objects would prove unacceptable to States.[421] However, the French example (*supra*, p. 59) shows that this is not *per se* true.[422] There is, however, also explicit *opinio iuris* to the contrary.[423]

95. To conclude, even though data is intangible, it may be targeted by attacks and it is susceptible to alteration and destruction.[424] If data is not considered an object, destroying valuable civilian data would fall outside the scope of protection of IHL, which would contradict the principle set out in article 48 AP I, to protect the civilian population from the effects of hostilities, and which would pose a considerable threat to the civilian society at large.[425] The inclusion of data as objects also has the benefit of providing clarity as to the identification of permissible military targets.[426] Nevertheless, the difference of the experts and States is not without good reason. At its broadest understanding, almost every

---

[416] ICRC Position Paper, 8; article 12 AP I.
[417] ICRC Position Paper, 8.
[418] R. GEISS and H. LAHMANN, "Protection of Data in Armed Conflict", *International Law Studies* 2021, Vol. 97, 556-572, 564.
[419] M. SCHMITT, "The Notion of 'Objects' During Cyber Operations: A Riposte in Defence of Interpretive and Applicative Precision", *Israel Law Review* 2015, Vol. 48(1), 81-109.
[420] K. MACAK, "Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law", *Israel Law Review* 2015, Vol. 48(1), 55-80, 73-74; N. LUBELL, "Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply?", *International Law Studies* 2013, Vol. 89, 252-275, 263.
[421] M. SCHMITT, "Wired warfare 3.0: Protecting the civilian population during cyber operations", *International Review of the Red Cross* 2019, Vol. 101(1), 333-355, 353.
[422] Ministère des Armées de France, Droit International Applique aux Operations dans le Cyberspace, 14-15; M. SCHMITT, "France Speaks Out on IHL and Cyber Operations: Part II", 1 October 2019, *EJIL:Talk!*, available at: https://www.ejiltalk.org/france-speaks-out-on-ihl-and-cyber-operations-part-ii/.
[423] Inter-American Juridical Committee, *International Law and State Operations*, 2020, 48, available at:
http://www.oas.org/en/sla/iajc/docs/International_Law_and_State_Cyber_Operations_publication.pdf.
[424] K. MACAK, "Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law", *Israel Law Review* 2015, Vol. 48(1), 55-80, 55.
[425] K. MACAK, "Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law", *Israel Law Review* 2015, Vol. 48(1), 55-80, 59; R. GEISS and H. LAHMANN, "Protection of Data in Armed Conflict", *International Law Studies* 2021, Vol. 97, 556-572, 571
[426] K. MACAK, "Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law", *Israel Law Review* 2015, Vol. 48(1), 55-79.

type of cyber operation is by definition targeting data.[427] While understanding the caution on including data as IHL objects, the author sees no solid reason put forward for its exclusion. Certainly not for content-level data. Nevertheless, content-level data may be better protected under international human rights law.[428] In relation to operational-level data, the author proposes a consequence-based approach. This is in line with both the *ratio legis* and the application of IHL and the position of the ICRC. This is also similar to the position of the Tallinn Manual that an operation against data which foreseeably results in the injury or death of individuals or damage or destruction of physical objects, must be regarded as an operation targeting those individuals or physical objects.[429]

c. Proportionality

96. Article 51(5)(b) of the Additional Protocol I states that an attack is prohibited if it may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated.[430] In short, the principle of proportionality concerns so-called collateral damage and seeks to limit excessive and avoidable civilian harm.[431] As highlighted earlier, with most cyber infrastructure being dual-use, the principle of proportionality is paramount for the protection of civilians and civilians objects in situations of cyber armed conflict.[432]

97. Importantly, the principle of proportionality requires an *ex ante* analysis.[433] The standard of adherence is that of a reasonable commander in the circumstances known at the moment of the launch of the attack.[434] Practically, it is about taking into account the consequences that are reasonably expected to occur and to avoid *excessive* civilian harm.[435] This is a very difficult exercise to make, for example forcing a comparison between civilian lives and a particular military objective.[436] On the other hand, even exceedingly extensive civilian

---

[427] R. GEISS and H. LAHMANN, "Protection of Data in Armed Conflict", *International Law Studies* 2021, Vol. 97, 556-572, 569.
[428] R. GEISS and H. LAHMANN, "Protection of Data in Armed Conflict", *International Law Studies* 2021, Vol. 97, 556-572, 570.
[429] Tallinn Manual 2.0, 416.
[430] Art. 51(5)(b) AP I.
[431] Tallinn Manual 2.0, 471.
[432] Z. CHANG, "Cyberwarfare and International Humanitarian law", *Creighton International and Comparative Law Journal* 2017, Vol. 9(1), 29-53, 41.
[433] P. PASCUCCI, "Distinction and Proportionality in Cyber War: Virtual Problems with a Real Solution", *Minnesota Journal of International Law* 2017, Vol. 26(2), 419-460, 446.
[434] P. PASCUCCI, "Distinction and Proportionality in Cyber War: Virtual Problems with a Real Solution", *Minnesota Journal of International Law* 2017, Vol. 26(2), 419-460, 446.
[435] As Yoram Dinstein puts it eloquently: "*Injury/damage to non-combatants can be exceedingly extensive without being excessive*": Y. DINSTEIN, "Discussion: Reasonable Military Commanders and Reasonable Civilians" in E. WALL (ed.), *International Law Studies – Legal and Ethical Lessons of NATO's Kosovo Campaign*, Newport, Naval War College, 2002, 173-219, 177; G. D. SOLIS, *The Law of Armed Conflict: International Humanitarian Law in War*, Cambridge, Cambridge University Press, 2016, 300.
[436] M. SASSOLI, *International Humanitarian Law: Rules, Controversies, and Solutions to Problems Arising in Warfare*, Cheltenham, Edward Elgar Publishing, 2019, 362.

damage does not make the attack automatically disproportionate when it is not excessive in light of an important military objective.[437] For example, a cyberattack on the Global Positioning System (GPS), which is dual-use, is not necessarily prohibited despite the severe harmful consequences for civilians and civilian objects that it would have.[438]

98. The Tallinn Manual argues that any expected direct and indirect effects must be factored into the proportionality analysis.[439] However, it is clear that not every civilian inconvenience must be considered.[440] Because the principle obliges the attacker to take into account damage to civilian objects, the qualification discussion on data is also relevant for its application. The loss of functionality is not an element that is listed for consideration in the proportionality assessment.[441] For this reason, some authors argue that 'damage' would not only include physical damage, but also the loss of functionality.[442] While it would seem logical in line with previous points, it does not seem like State practice has adopted such extensions of the principle of proportionality.[443]

99. In the opinion of the author, the current understanding of proportionality and the effects to consider may create a risk whereby cyber harm always 'loses' the proportionality analysis.[444] After all, cyberattacks are often perceived as less harmful than their kinetic counterparts.[445] This disregards more long-term harmful consequences, such as leaks, spill-overs or repurposing of the cyber tools by malevolent actors. The situation is furthermore suboptimal because it leaves the protection of civilians and civilian objects to a large degree (per the prevailing view, for all dual-use cyber infrastructure) to the scrutiny of the attacker. Indeed, the principle of proportionality is not only hard to apply but

---

[437] S. VERHOEVEN, "The Protection of Civilians and Civilian Objects Against Hostilities" in J. WOUTERS, P. DE MAN and N. VERLINDEN (eds.), *Armed Conflicts and the Law*, Mortsel, Intersentia, 2016, 259-303, 281; Y. DINSTEIN, "Discussion: Reasonable Military Commanders and Reasonable Civilians" in E. WALL (ed.), *International Law Studies – Legal and Ethical Lessons of NATO's Kosovo Campaign*, Newport, Naval War College, 2002, 173-219, 177.

[438] Tallinn Manual 2.0, 471-472.

[439] Tallinn Manual 2.0, 472; P. PASCUCCI, "Distinction and Proportionality in Cyber War: Virtual Problems with a Real Solution", *Minnesota Journal of International Law* 2017, Vol. 26(2), 419-460, 450.

[440] P. PASCUCCI, "Distinction and Proportionality in Cyber War: Virtual Problems with a Real Solution", *Minnesota Journal of International Law* 2017, Vol. 26(2), 419-460, 447.

[441] R. GEISS and H. LAHMANN, "Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space", *Israel Law Review* 2012, Vol. 45(3), 381-399, 397.

[442] C. DROEGE, "Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians", *International Review of the Red Cross* 2012, Vol. 94(886), 571; R. GEISS and H. LAHMANN, "Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space", *Israel Law Review* 2012, Vol. 45(3), 381-399, 399.

[443] W. BANKS, "Who Did It? Attribution of Cyber Intrusions and the Jus In Bello" in R. T. P. ALCALA and E. T. JENSEN (eds.), *The Impact of Emerging Technologies on the Law of Armed Conflict*, Oxford, Oxford University Press, 2019, 235-272, 257.

[444] See for example: J. A. RABKIN and J. YOO, *Striking Power: How Cyber. Robots and Space Weapons Change the Rule for War*, New York, Encounter Books, 2017, 156.

[445] J. KELSEY, "Hacking into international humanitarian law: the principle of distinction and neutrality in the age of cyber warfare", *Michigan Law Review* 2008, Vol. 106(7), 1435.

also susceptible to subjective value judgments, even for a reasonable commander.[446]

d. Precaution

100. Articles 57 and 58 of Additional Protocol I require parties to an armed conflict to adopt precautionary measures to protect civilian populations and objects against the effects of attacks.[447] The principle of precaution covers both active precaution (precaution in attack) and passive precaution (precaution against the effect of attacks).

101. Active precaution means that constant care must be taken to spare the civilian population or civilian objects.[448] SCHMITT highlights that this specific obligation does not require the 'attack' threshold and argues that the duty of 'constant care' will be especially relevant in situations of cyber armed conflict.[449] Secondly, the attacker must verify that targets of attacks are really military objectives.[450] For this reason, both attacking- and victim States would benefit from a clear framework distinguishing military and civilian cyber objects. In practical terms, precaution in cyberspace may include mapping the network of the adversary.[451] Importantly, if the available information is incomplete, the scope of the attack might have to be limited to only those targets on which there is insufficient information.[452]

102. The active precaution exercise also has implications on the choice of means or methods of warfare and how they are used.[453] Furthermore, precaution also entails a continuing obligation to assess proportionality and to adapt, suspend or terminate the cyberattacks accordingly.[454] Per article 57(3) AP I, precaution also affects the choice of targets: if there are multiple equivalent objectives, the one which may be expected to cause the least danger to civilians and civilian objects

---

[446] M. SASSOLI, *International Humanitarian Law: Rules, Controversies, and Solutions to Problems Arising in Warfare*, Cheltenham, Edward Elgar Publishing, 2019, 362.
[447] A. COCO and T. D. S. DIAS, "'Cyber Due Diligence': A Patchwork of Protective Obligations in International Law", *European Journal of International Law* 2021, 1-35, 33.
[448] Art. 57(1) AP I; ICRC Customary International Humanitarian Law Study, Rule 15, available at: https://ihl-databases.icrc.org/customary-ihl/eng/docindex/v1_rul_rule15.
[449] M. SCHMITT, "Wired warfare 3.0: Protecting the civilian population during cyber operations", *International Review of the Red Cross* 2019, Vol. 101(1), 333-355, 354.
[450] Art. 57(2)(a)(i) AP I; ICRC Customary International Humanitarian Law Study, Rule 16, available at: https://ihl-databases.icrc.org/customary-ihl/eng/docindex/v1_rul_rule16; Tallinn Manual 2.0, 478.
[451] C. DROEGE, "Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians", *International Review of the Red Cross* 2012, Vol. 94(886), 573.
[452] Tallinn Manual 2.0, 479.
[453] Article 57(2)(a)(ii) AP I; Tallinn Manual 2.0, 479-480; ICRC Customary International Humanitarian Law Study, Rule 16, available at: https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule16; S. VERHOEVEN, "The Protection of Civilians and Civilian Objects Against Hostilities" in J. WOUTERS, P. DE MAN and N. VERLINDEN (eds.), *Armed Conflicts and the Law*, Mortsel, Intersentia, 2016, 259-303, 282.
[454] Tallinn Manual 2.0, 481, 483; S. VERHOEVEN, "The Protection of Civilians and Civilian Objects Against Hostilities" in J. WOUTERS, P. DE MAN and N. VERLINDEN (eds.), *Armed Conflicts and the Law*, Mortsel, Intersentia, 2016, 259-303, 283.

is to be selected.[455] The customary status of this obligation is doubtful.[456] An interesting question is the duty of warning under article 57(2)(c) of AP I: attackers are obliged to give effective advance warning if the attacks may affect the civilian population, unless circumstances do not permit.[457] The obligation does not apply to attacks damaging civilian objects and not harming any persons. The warning must allow the intended recipient sufficient time to act.[458] However, if the attack requires surprise, no warning is needed. Given the instantaneous and covert nature of cyber operations, having to give effective warning in advance might render them useless. Therefore, it would seem that most States will argue that their attack affecting civilian population requires surprise to avoid the duty of warning.

103. Passive precaution means that the targeted State is required to take feasible measures to protect its civilians and civilian objects.[459] Traditionally, this can be done by not locating military targets within or near densely populated areas and by removing civilian persons and objects from the vicinity of military targets.[460] In cyberspace, this may be done by segregating military and civilian cyber infrastructure, by digitally flagging them or even by backing-up civilian data.[461] It must be noted that passive precaution does not prohibit dual-use.[462] Perhaps the recent example of the United States and Russia trying to agree on cyber safe zones could be seen as an application of passive precaution, or even as the cyber analogy of a demilitarised zone under article 60 AP I.[463]

104. Clearly, the principle of precaution has a lot of practical implications for both the attacker- and attacked State. While cyber operations may specifically target military infrastructure, they have the potential to indiscriminately disable civilian infrastructure or disrupt the provision of essential civilian services.[464] States may thus be required to adopt measures like separating between military and civilian cyberinfrastructure and networks, and identifying and protecting

---

[455] S. VERHOEVEN, "The Protection of Civilians and Civilian Objects Against Hostilities" in J. WOUTERS, P. DE MAN and N. VERLINDEN (eds.), *Armed Conflicts and the Law*, Mortsel, Intersentia, 2016, 259-303, 283.
[456] Tallinn Manual 2.0, 482.
[457] Tallinn Manual 2.0, 484-485; M. SASSOLI, *International Humanitarian Law: Rules, Controversies, and Solutions to Problems Arising in Warfare*, Cheltenham, Edward Elgar Publishing, 2019, 365.
[458] Tallinn Manual 2.0, 485.
[459] M. SASSOLI, *International Humanitarian Law: Rules, Controversies, and Solutions to Problems Arising in Warfare*, Cheltenham, Edward Elgar Publishing, 2019, 367.
[460] H. LIN, "Cyber Conflict and International Humanitarian Law", *International Review of the Red Cross* 2012, 886(94), 526.
[461] R. GEISS and H. LAHMANN, "Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space", *Israel Law Review* 2012, Vol. 45(3), 381-399, 392.
[462] S. VERHOEVEN, "The Protection of Civilians and Civilian Objects Against Hostilities" in J. WOUTERS, P. DE MAN and N. VERLINDEN (eds.), *Armed Conflicts and the Law*, Mortsel, Intersentia, 2016, 259-303, 284.
[463] "Biden tells Putin certain cyberattacks should be 'off-limits'", 17 June 2021, available at: https://www.reuters.com/technology/biden-tells-putin-certain-cyber-attacks-should-be-off-limits-2021-06-16/.
[464] A. COCO and T. D. S. DIAS, "'Cyber Due Diligence': A Patchwork of Protective Obligations in International Law", *European Journal of International Law* 2021, 1-35, 30-31, and DOI: https://doi.org/10.1093/ejil/chab056.

critical civilian infrastructure and services.[465] To be of any use, such precautionary duties extend beyond times of armed conflict. States are well-advised to agree on safe zones and to segregate their military and civilian cyber infrastructure in so far as reasonably and feasibly possible. From a technical point of view, this is easier said than done.[466]

e. Cyber means and methods of warfare

105. Per article 35 AP I, States are limited in their choice of means and methods of warfare. Article 36 AP I states that in the development, acquisition or adoption of a new weapon, means or method of warfare, a State is under an obligation to determine whether its employment would be prohibited by the Additional Protocol or any other rule of international law applicable to the State.[467] States bear this obligation for cyber means/weapons they themselves develop or design and for those that they acquire.[468] In this context it must also be reminded that indiscriminate cyber means are prohibited.[469] Clearly, a State using cyber means/weapons that are developed to self-propagate indiscriminately would not only be prohibited by IHL but also violate that State's obligation to review.[470] A concrete proposal could be the adoption of a new Protocol to the 1980 Convention on Certain Conventional Weapons, dedicated to self-propagating cyber tools, because of their indiscriminate nature.[471]

2.3.4. Conclusion

106. Applying IHL to situations of cyber conflict seems appealing because of its capacity to protect civilians and civilian objects. However, much of that potential goes lost when trying to apply IHL to cyber operations. Even if cyber operations alone can amount to an armed conflict, they individually have to constitute 'attacks' to be regulated by important IHL rules on the conduct of hostilities. Both are, however, not inconceivable under a kinetic effects equivalency test. On dual-use cyber infrastructure, the paper has stressed the importance of

---

[465] A. COCO and T. D. S. DIAS, "'Cyber Due Diligence': A Patchwork of Protective Obligations in International Law", *European Journal of International Law* 2021, 1-35, 34, and DOI: https://doi.org/10.1093/ejil/chab056; Tallinn Manual 2.0, 478.

[466] For an overview of concrete proposals, see: ICRC, *The Potential Human Cost of Cyber Operations*, ICRC Expert Meeting, 16-18 November 2018, Geneva, 39-42 and 75-77; see also the Natanz nuclear facility which was air-gapped (disconnected from other networks) and still got hit by the Stuxnet virus via a USB.

[467] Article 36 AP I; Tallinn Manual 2.0, 464; see also the 2006 ICRC guide on the implementation of article 36 AP I, available at: https://www.icrc.org/en/doc/assets/files/other/irrc_864_icrc_geneva.pdf.

[468] Tallinn Manual 2.0, 465.

[469] ICRC Position Paper, 5; ICRC Customary International Humanitarian Law Study, Rule 71, available at: https://ihl-databases.icrc.org/customary-ihl/eng/docindex/v1_rul_rule71.

[470] ICRC, *International Humanitarian Law and the Challenges of Contemporary Conflicts*, Geneva, 2019, 28, available at: https://shop.icrc.org/international-humanitarian-law-and-the-challenges-of-contemporary-armed-conflicts-recommitting-to-protection-in-armed-conflict-on-the-70th-anniversary-of-the-geneva-conventions-pdf-en.

[471] Convention On Prohibitions Or Restrictions On The Use Of Certain Conventional Weapons Which May Be Deemed To Be Excessively Injurious Or To Have Indiscriminate Effects As Amended On 21 December 2001, 10 October 1980.

applying the three-step test of article 52(2) AP I. On data protection in armed conflict, the paper has argued that data is not necessarily to be excluded from qualifying as objects but that adopting a consequence-based approach or seeking protection under international human rights law is perhaps a better solution. The author agrees with SCHMITT that the precautionary duty of constant care can be very meaningful to offer protection in cyber armed conflicts.[472] While further clarifying essential aspects such as the article 52(3) AP I presumption, or adopting specific instruments on establishing safe zones or to prohibit indiscriminate cyber means, a cyber-specific Additional Protocol is not necessary.[473]

2.4 HUMAN RIGHTS IN INTERNATIONAL CYBER CONFLICTS

2.4.1. Introduction

107. It is widely recognised internationally that individuals enjoy the same human rights online as they enjoy offline.[474] More than 180 governments have reaffirmed the full applicability of the Universal Declaration of Human Rights online.[475] In other words, the enjoyment of human rights cannot depend on the medium on which one wishes to exercise them. Perhaps the most relevant human rights in a cyber conflict scenario are the right to privacy and the right to data protection.[476] However, cyber operations may also cause damage or destruction to property.[477] It is also not inconceivable that cyber operations infringe upon the right to life, for example in instances where essential civil infrastructures are implicated.

108. It must be highlighted that far from all human rights law enjoys the recognition as customary international law. As a consequence, States mostly bear obligations only for those human rights that are included in the treaties that they have signed and ratified, and under their respective understandings and limitations. This paper mainly focuses on two human rights instruments: the

---

[472] M. SCHMITT, "Wired warfare 3.0: Protecting the civilian population during cyber operations", *International Review of the Red Cross* 2019, Vol. 101(1), 333-355, 354.

[473] For a proposal on a cyber-specific Additional Protocol, see: P. PASCUCCI, "Distinction and Proportionality in Cyber War: Virtual Problems with a Real Solution", *Minnesota Journal of International Law* 2017, Vol. 26(2), 419-460, 454.

[474] Human Rights Council, A/HRC/32/L.20, The Promotion, Protection and Enjoyment of Human Rights on the Internet, 27 June 2016; UN General Assembly Res. 69/166, The Right to Privacy in the Digital Age, at 3 (Dec. 18, 2014); UN General Assembly, Resolution 68/167 on the right to privacy in the digital age, *UN Doc. A/RES/68/167*, 21 January 2014; Human Rights Council, Resolution 32/13, *UN Doc. A/HRC/RES/32/13*, 1 July 2016; B. VAN SCHAACK, "The United States' Position on the Extraterritorial Application of Human Rights Obligations: Now Is the Time for Change" *International Law Study* 90, 21-22.

[475] World Summit on the Information Society, WSIS-03/GENEVA/DOC/4-E, Declaration of Principles – Building the Information Society: a global challenge in the new Millennium, 12 December 2003, https://www.itu.int/net/wsis/docs/geneva/official/dop.html.

[476] Article 8 European Convention on Human Rights; Article 17 International Covenant on Civil and Political Rights; UN General Assembly, Resolution 68/167 on the right to privacy in the digital age, *UN Doc. A/RES/68/167*, 21 January 2014.

[477] F. DELERUE, *Cyber Operations and International Law*, Cambridge, Cambridge University Press, 2020, 269.

European Convention on Human Rights (ECHR) and the International Covenant on Civil and Political Rights (ICCPR). State parties are required to respect, protect and fulfil human rights.[478] There are two main challenges for an effective protection of human rights during a cyber conflict. First, there is the issue of concurrent application of international human rights law and IHL. Secondly, there is the issue of extraterritorial application of international human rights instruments to cyberspace situations.

2.4.2. Human rights during cyber armed conflict

109. During an armed conflict, civilians and their rights are protected by specific rules of IHL. However, some important civilian rights may be at risk during a cyber armed conflict that are not effectively protected under the IHL framework. Thus, the question is to what degree such rights enjoy protection under international human rights law during a cyber armed conflict. The relationship between human rights and IHL is a much debated one.[479] The ICJ in *Nuclear Weapons* and *Construction of a Wall* applied a *lex specialis* approach for IHL.[480] But it is not crystal clear how this should be applied case by case. For example, it is uncertain whether IHL overrules international human rights law during armed conflicts, or whether it serves as a means of interpretation of human rights obligations. In *Georgia v Russia (II)*, the ECtHR confirms, by reference to the *Hassan* judgment, that the safeguards under the Convention continue to apply in situations of international armed conflict, albeit interpreted against the background of the provisions of international humanitarian law.[481] This understanding is influenced by the caselaw of the ICJ.[482] Consequently, the author agrees with the principle that human rights continue to apply during armed conflicts. It also seems that the human rights bodies make use of IHL as a *lex specialis* to offer the highest level of protection, not to undermine human rights.[483]

---

[478] Human Rights Committee, General Comment No. 31: The Nature of the General Legal Obligations Imposed on States Parties to the Covenant, 6, *UN Doc.* CCPR/C/21/Rev.1/Add.13, 29 March 2004, paragraph 6; International Covenant on Economic, Social and Cultural Rights, art. 2.

[479] See for example: R. ARNOLD and N. QUENIVET (eds.), *International Humanitarian Law and Human Rights Law: Towards a New Merger in International Law*, The Hague, Martinus Nijhof, 2008, 587.

[480] ICJ, Legality of the use by a State of nuclear weapons in armed conflict, Advisory opinion, *I.C.J. Rep.* 1996, paragraph 25; ICJ, Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory opinion, *I.C.J. Rep.* 2004, paragraphs 106 and 142.

[481] ECtHR (Grand Chamber), Georgia v. Russia (II), No. 38263/08, 21 January 2021, paragraph 93 (the case concerned the human rights consequences of the 2008 armed conflict between Russia and Georgia); ECtHR (Grand Chamber), Hassan v. U.K., No. 29750/09, 16 September 2014, paragraph 104 (the case concerned the deprivation of liberty of an Iraqi person by U.K. armed troops during active hostilities in Iraq).

[482] ECtHR (Grand Chamber), Georgia v. Russia (II), No. 38263/08, 21 January 2021, paragraph 93; ECtHR (Grand Chamber), Hassan v. U.K., No. 29750/09, 16 September 2014, paragraph 102.

[483] F. NAERT, "Human Rights and (Armed) Conflict" in J. WOUTERS, P. DE MAN and N. VERLINDEN (eds.), *Armed Conflicts and the Law*, Mortsel, Intersentia, 2016, 212.

110. It is true that most human rights can be derogated from to some degree, they are not absolute.[484] In addition, general derogations are possible for human rights instruments. For example, the ECHR provides in its article 15 for a general derogation from the Convention that can be invoked by the State in times of war and public emergency.[485] This raises some questions concerning the relation between IHL and international human rights law. In *Hassan v. UK*, the ECtHR explicitly accepted a form of tacit derogation based on article 15 ECHR when IHL applies in international armed conflicts.[486] The ECtHR also seems to grant States a rather wide margin of appreciation in claiming the derogation under article 15 ECHR.[487] On its part, the ICCPR provides for a very similar derogation "*in time of public emergency which threatens the life of the nation and the existence of which is officially proclaimed*".[488] Both the ICCPR and the ECHR prohibit derogations that are not strictly required by the exigencies of the situations. Derogations inconsistent with the State's other international legal obligations are prohibited as well. Finally, certain human rights are non-derogable.[489]

2.4.3. Extraterritorial application in cyberspace

a. Principles of the ECHR and the ICCPR

111. The issue of extraterritorial application is of cardinal importance in cyberspace, where violations can easily occur without any territorial link or control, leaving victims without redress.[490] Under the ECHR, States bear human rights obligations within their jurisdiction.[491] The ICCPR proclaims that States have the obligation to respect and to ensure the rights in the Covenant to all individuals within their territory and subject to their jurisdiction.[492] Concerning the State's negative obligation to refrain from violating the ICCPR, the conditions are understood in a disjunctive sense: either when acts are within their territory or within their jurisdiction.[493] In *Burgos v. Uruguay*, the Human Rights

---

[484] Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms; The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981, *European Treaty Series*, no. 108.
[485] Art. 15 of the European Convention for the Protection of Human Rights and Fundamental Freedoms.
[486] ECtHR (Grand Chamber), Hassan v. United Kingdom, Application no. 29750/09, 2014, paragraph 104.
[487] F. NAERT, "Human Rights and (Armed) Conflict" in J. WOUTERS, P. DE MAN and N. VERLINDEN (eds.), *Armed Conflicts and the Law*, Mortsel, Intersentia, 2016, 193.
[488] ICCPR art. 4(1); ECHR art. 15(1); ACHR art. 27.
[489] Tallinn Manual 2.0, 208.
[490] F. DELERUE, *Cyber Operations and International Law*, Cambridge, Cambridge University Press, 2020, 263.
[491] Art. 1 of the European Convention for the Protection of Human Rights and Fundamental Freedoms.
[492] Art. 2(1) International Covenant on Civil and Political Rights.
[493] Human Rights Committee, General Comment No. 31: The Nature of the General Legal Obligations Imposed on States Parties to the Covenant, 6, *UN Doc.* CCPR/C/21/Rev.1/Add.13, 29 March 2004, paragraph 10.

Committee decided that extraterritorial application of the ICCPR is possible.[494] In *Construction of a Wall*, the ICJ found that the *travaux préparatoires* of the ICCPR show that the intention was not to allow States to escape responsibility when exercising jurisdiction outside of their territory.[495] Comparably, the ECtHR holds that article 1 ECHR cannot be interpreted in such a way that allows a State to commit violations of the ECHR outside of its territory which it would not be allowed to commit on its own territory.[496] Despite the controversial ECtHR *Bankovic* caselaw, extraterritorial application of the Convention is possible, albeit only by way of exception.[497] Evidently, not all States agree on the possibility of extraterritorial application of human rights instruments.[498]

b. Defining jurisdiction

112. The caselaw of extraterritorial application of the ECHR has been a dynamic one and revolves around the notion of 'jurisdiction'. The bottom line is that extraterritorial application is possible, but that it must remain an exception. The ECtHR has two models of jurisdiction, which it does not consistently apply. The first is that of personal jurisdiction: a State bears human rights obligations if a State exercises "*power or effective control*" over persons.[499] This is mostly understood as a requirement for physical control or custody over the person, such as in a situation of detention, as was decided in the ECtHR *Al-Skeini* case.[500] The second model is that of territorial jurisdiction, developed in the ECtHR *Louizidou* case: a State bears human rights obligations if a State exercises effective control, directly or indirectly, over an area outside its national territory.[501] This generally refers to situations of occupied territory. Comparably, the Human Rights Committee holds that the ICCPR applies extraterritorially

---

[494] Human Rights Committee, Burgos v. Uruguay, No. 52/1979, 29 July 1981, paragraphs 12.1-12.3 (the case concerned the abduction, torture and ill-treatment of Mr. Lopez Burgos, a Uruguayan political refugee residing in Argentina); K. KITTICHAISAREE, "Public International Law of Cyber Space", *Law, Governance and Technology Series* 2017, Vol. 32, 135 and DOI: 10.1007/978-3-319-54657-5.

[495] ICJ, Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, *I.C.J.Rep. 2004*, paragraphs 108–111.

[496] ECtHR, Issa and Others v. Turkey, No. 31821/96, 16 November 2004, paragraph 71 (the case concerned the responsibility of Turkey for alleged killings of shepherd by Turkish military in Northern Iraq); ECtHR, Solomou and Others v. Turkey, No. 36832/97, 24 June 2008, paragraph 45 (the case concerned the extrajudicial killing of Mr. Solomou on the occupied territory by Turkish forces in Northern Cyprus).

[497] ECtHR (Grand Chamber), Bankovic v. Belgium and Others, No. 52207/99, 12 December 2001 (the case concerned complaints on the human rights consequences of the NATO bombings in Belgrade, which the court dismissed as falling outside the scope of jurisdiction of the responsible States).

[498] G. RONA and L. AARONS, "State Responsibility to Respect, Protect and Fulfill Human Rights Obligations in Cyberspace", *Journal of National Security Law and Policy* 2016, Vol. 8, 503-530.

[499] F. NAERT, "Human Rights and (Armed) Conflict" in J. WOUTERS, P. DE MAN and N. VERLINDEN (eds.), *Armed Conflicts and the Law*, Mortsel, Intersentia, 2016, 203.

[500] ECtHR, Al-Skeini and Others v. United Kingdom, No. 55721/07, 7 July 2011, paragraph 136 (the case concerned extrajudicial killings of Iraqi civilians by U.K. armed troops in Basra, where the U.K. was the occupying power).

[501] ECtHR (Grand Chamber), Louizidou v. Turkey, 40/1993/435/514, 18 December 1996 (the court held Turkey responsible for the denial of ownership and the use of property of Ms. Louizidou over her house in Northern Cyprus, because she was refused entry by the Turkish army to the occupied territory when trying to return home).

"*to anyone within the power or effective control*" of the State.[502] This includes both *de facto* and *de iure* power or effective control, taking into account the circumstances of each case.[503]

113. In their simplest sense, these models suggest that a State would be bound to respect the human rights of individuals in cyberspace whenever these individuals are within its territory, in territory under its control, or when the individual is in the hands of a State agent.[504] These models are clearly predicated on physical situations. The Tallinn Manual could not achieve consensus on a proper application of these models in cyberspace, which is criticised.[505] This also means that the Tallinn Manual remains indecisive on the question whether control (over a person or over a territory) can be exercised by virtual means alone. Moreover, even if it would be possible, it remains unclear whether a State's control over a territory or a person through cyber means alone triggers the application of international human rights law.[506]

c. A functional approach to jurisdiction

c.1. Critique

114. In the classic understanding of extraterritoriality, States engaged in a cyber conflict do not bear any responsibility to protect human rights outside of their territory, since the States are not exercising control over a territory or over persons. Indeed, it seems that in the current state of the law *physical* control over territory or individuals is required before human rights law obligations are triggered.[507] This would mean that the threshold of control is never met in standalone cyber operations, so that important human rights remain unprotected. Thus, the existing theories of extraterritorial application risk being inapt for cyberspace, since they are predicated on physical elements that are simply not present for cyber operations. However, cyber operations can

---

[502] K. KITTICHAISAREE, "Public International Law of Cyber Space", *Law, Governance and Technology Series* 2017, Vol. 32, 135 and DOI: 10.1007/978-3-319-54657-5; Human Rights Committee, General Comment No. 31: The Nature of the General Legal Obligations Imposed on States Parties to the Covenant, 6, *UN Doc.* CCPR/C/21/Rev.1/Add.13, 29 March 2004, paragraph 10.

[503] K. KITTICHAISAREE, "Public International Law of Cyber Space", *Law, Governance and Technology Series* 2017, Vol. 32, 135 and DOI: 10.1007/978-3-319-54657-5, 135.

[504] G. RONA and L. AARONS, "State Responsibility to Respect, Protect and Fulfill Human Rights Obligations in Cyberspace", *Journal of National Security Law and Policy* 2016, Vol. 8, 508.

[505] *Tallinn Manual 2.0*, 185; see e.g. W. CONG, *Seeking Customary International Human Rights Law in the Cyberspace: A Critique of the Tallinn Manual 2.0*, 2018, available at: http://dx.doi.org/10.2139/ssrn.3744924; R. E. BARNSBY and S. R. REEVES, "Give Them an Inch, They'll Take a Terabyte: How States May Interpret *Tallinn Manual 2.0's* International Human Rights Law Chapter", *Texas Law Review* 2017, Vol. 95, 1515-1530.

[506] G. RONA and L. AARONS, "State Responsibility to Respect, Protect and Fulfill Human Rights Obligations in Cyberspace", *Journal of National Security Law and Policy* 2016, Vol. 8, 508.

[507] *Tallinn Manual 2.0*, 185; ECtHR (Grand Chamber), *Al-Skeini and others v. United Kingdom*, Application no. 55721/07, 2011, para 136.

accomplish the exact same results as physical operations and thus there seems to be no reason to treat them differently.[508]

115. More generally, there is critique on the narrow view of the 'control' test, namely where it is not triggered for as long as there is no physical control, because it leads to illogical results. Indeed, the very same State action that would be prohibited in the territory of the State would be permitted if committed beyond national borders.[509] This lies awkward with the proclaims of universal enjoyment of human rights. The protection of a human right would then depend on a purely factual criterium that is largely divorced from any normative evaluation of the interests at stake.[510] A narrow view of the 'control' test could lead to discrimination between citizens and foreigners, which should not be admissible according to the special UN Rapporteur on the right to privacy.[511] Also, looking at article 31 of the Vienna Convention on the Law of Treaties (VCLT) and the universalist normative foundation of human rights, an interpretation that values all human beings equally and is respectful of their individual dignity is inherently more preferable than one that does not.[512] Finally, in modern times the physical aspects of any individual may be located in a particular jurisdiction, but their rights, freedoms and identity increasingly reside where their data travels and can thus be subject to other States' control over them.[513]

c.2. Developments

116. Concerning the territorial model, the UN Office of the High Commissioner has taken the view that international human rights law applies where a State exercises power or effective control over digital communications infrastructure, wherever located, which would be the case with direct tapping or the penetration of communication structure.[514] While it is a welcome

---

[508] M. MILANOVIC, "Foreign Surveillance and Human Rights, Part 4: Do Human Rights Treaties Apply to Extraterritorial Interferences with Privacy?", *EJIL:TALK!*, 28 November 2013, available at: https://www.ejiltalk.org/foreign-surveillance-and-human-rights-part-4-do-human-rights-treaties-apply-to-extraterritorial-interferences-with-privacy/.

[509] F. BIGNAMI and G. RESTA, "Human Rights Extraterritoriality: The Right to Privacy and National Security Surveillance", *GW Legal Studies Research Paper No. 2017-67*, 5.

[510] F. BIGNAMI and G. RESTA, "Human Rights Extraterritoriality: The Right to Privacy and National Security Surveillance", *GW Legal Studies Research Paper No. 2017-67*, 5.

[511] Human Rights Council, Report of the Special Rapporteur on the right to privacy, *UN Doc. A/HRC/34/60*, 24 February 2017, paragraph 55.

[512] M. MILANOVIC, "Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age", *Harvard International Law Journal* 2015, Vol.56(1), 81-146, 109-110; ICJ, Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, *I.C.J.Rep. 2004*, paragraph 109.

[513] D. POKEMPER, "Cyberspace and State Obligations in the Area Of Human Rights" in K. ZJOLKOWSKI (ed.), *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy*, Tallinn, NATO CCD COE Publication, 2013, 239-260, 260.

[514] Human Rights Council, Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, *UN Doc. A/HRC/27/37*, 30 June 2014, paragraph 34; Human Rights Council, Report of the United Nations High Commissioner for Human Rights on the Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, Human Rights Council, *UN Doc. A/HRC/13/36*, Jan. 22 January 2010, 41.

development, it is also criticised because often its location is unrelated to that of the individuals whose human rights are at stake.[515] The ECtHR has found that a State may be in violation of the right to privacy when it intercepts personal data on its own territory that belongs to an individual situated outside of its territory.[516]

117. Concerning the personal model, MILANOVIC argued that it is not limited to situations of detention, but that it also covers killing, destruction of property and the invasion of privacy.[517] The argument that limiting the model to physical custody is arbitrary has gained recognition. The ECtHR has most recently confirmed in *Carter,* which concerned the alleged poisoning of Litvinenko by Russia in the United Kingdom, that the notion of physical power or control over an individual cannot be limited to situations of detention.[518] In relation to the right to life, the ECtHR takes a functional approach on jurisdiction: control over the (right to) life triggers the application of the ECHR obligations.[519] The reasoning in *Carter* expands on the ECtHR *Georgia v. Russia (II)* judgment, where the conclusions were limited to situations of 'proximate targeting'. That limitation was criticised as being arbitrary.[520] Importantly, the ECtHR decided in *Georgia v. Russia (II)* that the *Bankovic* logic against extraterritorial application of the ECHR applied during the time of armed conflict, arguing that an armed conflict happens in a context of chaos, meaning that both effective control over an area and State agent authority and control are excluded.[521]

118. Furthermore, MILANOVIC argues that reserving this functional logic to the right of life is arbitrary and that it would also apply to other ECHR rights.[522] This would mean that the implication of a human right by a State would potentially entail extraterritorial responsibility by that State. In other words, the duty to respect human rights would apply without any territorial limitation, since any act capable of violating that duty would be an exercise of control over the victim.[523] It must be noted that this only covers the 'negative' obligation for the State to respect human rights, i.e., not to violate them. It does not cover the

---

[515] M. MILANOVIC, "Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age", *Harvard International Law Journal* 2015, Vol.56(1), 81-146, 145.
[516] ECtHR, Liberty and Others v. United Kingdom, No. 58243/00, 1 July 2008 (the case concerned a successful complaint against UK legislation allowing surveillance and monitoring of communications).
[517] M. MILANOVIC, "Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age", *Harvard International Law Journal* 2015, Vol.56(1), 81-146, 115.
[518] ECtHR, Carter v. Russia, No. 20914/07, 21 September 2021, paragraphs 125-127 (the case concerned the alleged assassination of Mr. Litvinenko on U.K. territory with polonium).
[519] ECtHR, Carter v. Russia, No. 20914/07, 21 September 2021, paragraph 129.
[520] M. MILANOVIC, "European Court Finds Russia Assassinated Alexander Litvinenko", *EJIL:Talk!,* 23 September 2021, available at: https://www.ejiltalk.org/european-court-finds-russia-assassinated-alexander-litvinenko/.
[521] ECtHR (Grand Chamber), Georgia v. Russia (II), No. 38263/08, 21 January 2021, paragraph 137.
[522] M. MILANOVIC, "European Court Finds Russia Assassinated Alexander Litvinenko", *EJIL:Talk!,* 23 September 2021, available at: https://www.ejiltalk.org/european-court-finds-russia-assassinated-alexander-litvinenko/.
[523] M. MILANOVIC, "European Court Finds Russia Assassinated Alexander Litvinenko", *EJIL:Talk!,* 23 September 2021, available at: https://www.ejiltalk.org/european-court-finds-russia-assassinated-alexander-litvinenko/.

'positive' obligation for the State to secure or ensure human rights.[524] This is in line with the model that MILANOVIC famously proposed, whereby positive obligations for the State 'to ensure' are limited to its jurisdiction and negative obligations for the State 'to respect' would be territorially unlimited and not subject to any jurisdictional threshold.[525] This is also reflective of the disjunctive interpretation of art. 2(1) ICCPR by the Human Rights Committee for negative obligations (*supra*, p. 70).[526] Because States remain in full control of their own organs and agents, they are perfectly able to comply with negative obligations.[527] It further complies with the logic of universality of human rights.

119. The UN Office of the High Commissioner for Human Rights has also argued that a State's human rights obligations are triggered whenever it exercises regulatory jurisdiction over a third party that physically controls the personal data of individuals, or if a State asserts jurisdiction over the personal data of private companies as a result of the incorporation of those companies in the State.[528] In addition, the Human Rights Committee has raised concerns on the ICCPR implications of extraterritorial surveillance practices of the United States.[529] This indicates a growing affinity to extraterritoriality. In relation to the ICCPR right to life, the Human Rights Committee has formally taken a functional approach to extraterritorial jurisdiction, grounded in the exercise of control over the enjoyment of the rights in question, regardless of any physical control over the territory, the perpetrators or the individual victim.[530] This is not unlike the ECtHR *Carter* judgment. A comparable argument was entertained but disregarded in the Tallinn Manual. Some of the experts argued that so long as the exercise or enjoyment of a human right by an individual is within the power or effective control of a State, namely when the action of a State can obstruct such exercise or enjoyment, the State exercises power or effective control *in personam* over the individual and does bear extraterritorial human rights obligations.[531] A functional approach to jurisdiction can also be found in recent caselaw of the Inter-American Court of Human Rights, albeit in the area of transboundary environmental harm: "*it is understood that the persons whose rights have been violated are under the jurisdiction of the State of origin* [the

---

[524] M. MILANOVIC, *Extraterritorial application of Human Rights Treaties*, New York, Oxford University Press, 2011, 210.
[525] M. MILANOVIC, "Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age", *Harvard International Law Journal* 2015, Vol.56(1), 81-146, 119.
[526] Human Rights Committee, General Comment No. 31: The Nature of the General Legal Obligations Imposed on States Parties to the Covenant, 6, *UN Doc.* CCPR/C/21/Rev.1/Add.13, 29 March 2004, paragraph 10.
[527] M. MILANOVIC, "Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age", *Harvard International Law Journal* 2015, Vol.56(1), 81-146, 119; B. VAN SCHAACK, "The United States' Position on the Extraterritorial Application of Human Rights Obligations", *International Law Studies* 2014, Vol. 90, 49-52.
[528] Human Rights Council, Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, *UN Doc. A/HRC/27/37*, 30 June 2014, paragraph 34.
[529] Human Rights Committee, Concluding Observations on the Fourth Periodic Report of the United States, *UN Doc. CCPR/C/USA/CO/4*, 23 April 2014, 22.
[530] Human Rights Committee, General Comment No. 36 on Article 6 ICCPR: right to life, *CCPR/C/GC/36*, 3 September 2019, paragraph 63.
[531] *Tallinn Manual 2.0*, 185-186.

State under whose jurisdiction or control the causal activity originated] *if there is a causal link between the act that originated in its territory and the infringement of the human rights of persons outside its territory*".[532] Indeed, it is that State of origin that is in a position to prevent impacting the enjoyment of human rights of persons located outside its territory.[533]

120. Multiple authors have made proposals similar to that of functional jurisdiction. One argues that the extraterritorial State exercising effective control over crucial aspects of individual personality and autonomy can be understood as exercising jurisdiction for the purpose of international human rights law applicability.[534] Some authors argue for a test that is specific to the human right at issue.[535] This is a flexible approach, meaning that the concept of 'control' can be stretched or tightened depending on the circumstances of application. Such a flexible approach would then exist in cyberspace. For example, whenever a State collects personal data, it would indirectly be exercising control over those persons that generated the data, irrespective of the modalities or place of the collection or the nationality of the data subject.[536] Finally, there is also the argument the apply the alternative 'virtual control' in cyberspace (*supra*, p. 23).[537]

d. Non-State actors

121. The direct application of human rights law to non-State actors remains doubtful, but there is no doubt that States have an obligation not only to respect, but also to ensure respect for human rights by regulating the conduct of non-State actors.[538] As explained hereabove, the positive obligation of the State 'to ensure' is more rigidly limited to its territory under the ICCPR and ECHR. More generally, a State may be held responsible for human rights violations committed by non-State actors under the traditional conditions of State

---

[532] Inter-American Court of Human Rights, Advisory Opinion OC-23/17, 15 November 2017, paragraph 101 (the case concerned a request by Colombia on the legal implications of transboundary environmental consequences, specifically in relation to the maritime environment, caused by infrastructure projects).

[533] Inter-American Court of Human Rights, Advisory Opinion OC-23/17, 15 November 2017, paragraph 102.

[534] D. POKEMPNER, "Cyberspace and State Obligations in the Area of Human Rights" in K. ZIOLKOWSKI (ed.), *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy*, Tallinn, NATO CCD COE, 2013, 239-260, 259.

[535] F. BIGNAMI and G. RESTA, "Human Rights Extraterritoriality: The Right to Privacy and National Security Surveillance", *GW Legal Studies Research Paper No. 2017-67*, 5; M. MILANOVIC, "Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age", *Harvard International Law Journal* 2015, Vol.56(1), 81-146.

[536] M. MILANOVIC, "Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age", *Harvard International Law Journal* 2015, Vol.56(1), 81-146; P. MARGULIES, "The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism", *Fordham Law Review* 2014, Vol. 82, 2137; I. GEORGIEVA, "The Right to Privacy under Fire – Foreign Surveillance under the NSA and the GCHQ and Its Compatibility with Art. 17 ICCPR and Art. 8 ECHR" *Utrecht Journal of International and European Law* 2015, Vol.31(80), 104-13.

[537] P. MARGULIES, "The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism", *Fordham Law Review* 2014, Vol. 82, 2137.

[538] G. RONA and L. AARONS, "State Responsibility to Respect, Protect and Fulfill Human Rights Obligations in Cyberspace", *Journal of National Security Law and Policy* 2016, Vol. 8, 528.

attribution (*supra*, p. 19).[539] The ECtHR *Carter* judgment is also relevant here. It is one of the first cases in which the ECtHR explicitly applies article 8 of the ILC ARSIWA to find that the conduct of non-State actors was attributable to the State.[540] Very boldly however, the ECtHR established State responsibility by shifting the burden of proof and by drawing conclusions from Russia's lack of cooperation to provide the evidence to the contrary.[541] While it is based on inferential reasoning, it is justified by the specific facts of the case and by the functioning of the ECtHR.[542]

2.4.4. Conclusion

122. Because the classic approaches to jurisdiction are predicated on physical elements that are simply absent in situations of international cyber conflict, this author largely agrees with the position of MILANOVIC. If one wants to avoid a complete lack of redress under international human rights law for individual victims of cyber conflicts, one must accept that the existing set of rules is not apt and furthermore, largely arbitrary. A growing support for a functional approach to jurisdiction has been established. It remains to be seen whether this will remain confined within the right to life and situations of transboundary environmental harm. Logic and formulation would suggest otherwise.[543] A functional understanding of jurisdiction for extraterritorial negative obligations of States is necessary to ensure effective legal remedy for victims of international cyber conflicts. It merits emphasis that this is only concerned with admissibility and not with substance: implication does not automatically mean violation. Concerns about far-reaching extraterritorial obligations are thus misguided. States are simply obligated to refrain from violating human rights by cyber means outside of their territory as they are within their territory. If taken up by a court, minor or accidental extraterritorial consequences will most likely be remediated in the proportionality analysis, functioning as a *de minimis* threshold for State responsibility.

123. The question remains whether the ECtHR's 'chaos logic'[544] against extraterritorial application during armed conflicts would be applied to cyber armed conflicts as well. The logic is explicitly built upon the situation of physical armed confrontation and fighting that excludes the possibility of jurisdiction

[539] Tallinn Manual 2.0, 197.
[540] M. MILANOVIC, "European Court Finds Russia Assassinated Alexander Litvinenko", *EJIL:Talk!,* 23 September 2021, available at: https://www.ejiltalk.org/european-court-finds-russia-assassinated-alexander-litvinenko/.
[541] ECtHR, Carter v. Russia, No. 20914/07, 21 September 2021, paragraphs 72 and 166-169.
[542] M. MILANOVIC, "European Court Finds Russia Assassinated Alexander Litvinenko", *EJIL:Talk!,* 23 September 2021, available at: https://www.ejiltalk.org/european-court-finds-russia-assassinated-alexander-litvinenko/.
[543] See for example in *Carter*: "*Targeted violations of the human rights of an individual by one Contracting State in the territory of another Contracting State undermine the effectiveness of the Convention*". Note that it refers to "*violations of the human rights*" in plural, not limiting itself to the right to life. (ECtHR, Carter v. Russia, No. 20914/07, 21 September 2021, paragraph 128).
[544] ECtHR (Grand Chamber), Georgia v. Russia (II), No. 38263/08, 21 January 2021, paragraph 137.

under the territorial and personal model.[545] The different factual situation of a cyber armed conflict and the different nature of the functional model of jurisdiction may be reasons for distinction.

3. CASE STUDY

3.1. INTRODUCTION

124. The purpose of this part is to analyse a real-world cyber conflict. After a brief overview of the relevant facts, the conclusions and points from the previous chapters will be tested and applied. The conflict studied is that between in Israel and Iran. It is interesting for multiple reasons. Firstly, because of its 'cold' nature and mixture with kinetic operations.[546] Secondly, for its reliance on non-State actors and diversity in operations. Thirdly, because Israel is one of the most cyber-advanced States in the world.[547] Fourth, it lays bare how civilians and civilian infrastructure are particularly vulnerable to offensive cyber operations. Cyber tit-for-tats can easily escalate in terms of targets and magnitude, to the detriment of civilians and their rights.[548] Finally, it shows the futility of limiting a study of cyber conflict to one specific domain of international law. Frustrating as it may be the case study is perhaps most successful in showing the difficulties of application and the corresponding lack of protection.

3.2. OVERVIEW OF THE FACTS

125. Although there have recently been physical face-offs and drone strikes between the States in Syria and Lebanon, as well as in the Middle East shipping lanes[549], the 'cold'[550] cyber conflict between the two States at least dates back to the 2010 Stuxnet attack on Iranian nuclear infrastructure. The Stuxnet attack was famous as the first cyber operation ever to cause physical damage.[551] It is reported that the 2012 Shamoon attacks, which wreaked havoc in the Middle East, are linked to Iran.[552] Most recently, in fall 2021, a network of over 4.000

---

[545] ECtHR (Grand Chamber), Georgia v. Russia (II), No. 38263/08, 21 January 2021, paragraph 137: "*the very reality of armed confrontation and fighting between enemy military forces seeking to establish control over an area in a context of chaos not only means that there is no "effective control" over an area as indicated above (see paragraph 126 above), but also excludes any form of "State agent authority and control" over individuals.*".

[546] "Iran and Israel accuse each other of cyber-attacks in escalating 'Cold War'", 3 November 2021, available at: https://www.independent.co.uk/tech/iran-israel-cyber-lgbtq-leak-war-b1950673.html.

[547] International Institute for Strategic Studies, "Cyber Capabilities and National Power: a Net Assessment", *Research Papers*, 28 June 2021, available at: https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power.

[548] "Iran-Israel: the larger implications of cyber conflict", 19 September 2020, available at: https://www.strikesource.com/2020/09/19/iran-israel-the-larger-implications-of-cyber-conflict/.

[549] "Iran and Israel accuse each other of cyber-attacks in escalating 'Cold War'", 3 November 2021, available at: https://www.independent.co.uk/tech/iran-israel-cyber-lgbtq-leak-war-b1950673.html.

[550] "Iran and Israel accuse each other of cyber-attacks in escalating 'Cold War'", 3 November 2021, available at: https://www.independent.co.uk/tech/iran-israel-cyber-lgbtq-leak-war-b1950673.html.

[551] ICRC, "Iran, Victim of Cyber Warfare", https://casebook.icrc.org/case-study/iran-victim-cyber-warfare.

[552] "Shamoon computer virus variant is lead suspect in hack on oil form Saipem", 12 December 2018, available at: https://www.reuters.com/article/cyber-shamoon-idUSL1N1YH0QC.

fuel stations across Iran were sabotaged, resulting in fuel shortages.[553] In retaliation, private personal data from Israeli military and the Minister of Defence were leaked. Earlier in Israel, sensitive civilian medical data were leaked of 290.000 patients from several hospitals in Jerusalem. This accompanied an earlier leak of personal data, which included the HIV status, of users of an Israeli LGBTQ+ dating website.[554] In April 2021, there was a successful cyberattack on Iran's main nuclear facility, reminiscent of Stuxnet.[555] Back in April 2020, Israeli civilian water facilities were targeted, leading to the destruction of data and the taking-over of the pumps.[556] There was an attempt to change the chlorine levels of the water supply to Israeli homes.[557] In return, Iran's major shipping port, Shahid Rajaee, was shut down, massively disrupting maritime traffic for a couple of days.[558] In addition to these incidents, there were many reported cases of cyber espionage.[559] For example, Israel has claimed that it suffers cyber operations from Iran on a daily basis.[560] Iran has stated to reserve the right to respond against the ones responsible for the latest attacks.[561]

126. Within the OEWG, both States seem to agree on the general applicability of international law to cyberspace, while insisting on further clarification: in their communications, both States remain very cautious in their approach.[562] Neither

---

[553] "Iran and Israel accuse each other of cyber-attacks in escalating 'Cold War'", 3 November 2021, available at: https://www.independent.co.uk/tech/iran-israel-cyber-lgbtq-leak-war-b1950673.html.

[554] "'Black Shoadow hackers leak data from Israeli LGBT app", 31 October 2021, available at: https://www.jpost.com/israel-news/iranian-hackers-breach-israeli-company-cyberserve-683529.

[555] "Israel appears to confirm it carried out cyberattack on Iran nuclear facility", 11 April 2021, available at: https://www.theguardian.com/world/2021/apr/11/israel-appears-confirm-cyberattack-iran-nuclear-facility; "Iran says key Natanz nuclear facility hit by 'sabotage'", 12 April 2021, available at: https://www.bbc.com/news/world-middle-east-56708778.

[556] "Iran-Israel: the larger implications of cyber conflict", 19 September 2020, available at: https://www.strikesource.com/2020/09/19/iran-israel-the-larger-implications-of-cyber-conflict/; "Israeli footprints in Iran: cyberattacks, targeted killings, more", 26 April 2021, available at: https://www.aa.com.tr/en/middle-east/israeli-footprints-in-iran-cyberattacks-targeted-killings-more/2220652; Council on Foreign Relations Report, "Attack on Israeli water utilities", May 2020, available at: https://www.cfr.org/cyber-operations/attack-israeli-water-utilities.

[557] "Iran-Israel: the larger implications of cyber conflict", 19 September 2020, available at: https://www.strikesource.com/2020/09/19/iran-israel-the-larger-implications-of-cyber-conflict/;"Israeli footprints in Iran: cyberattacks, targeted killings, more", 26 April 2021, available at: https://www.aa.com.tr/en/middle-east/israeli-footprints-in-iran-cyberattacks-targeted-killings-more/2220652; "Israel and Iran Just Showed Us the Future of Cyberwar With Their Unusual Attacks", 5 June 2020, available at: https://foreignpolicy.com/2020/06/05/israel-and-iran-just-showed-us-the-future-of-cyberwar-with-their-unusual-attacks/.

[558] "Iran-Israel: the larger implications of cyber conflict", 19 September 2020, available at: https://www.strikesource.com/2020/09/19/iran-israel-the-larger-implications-of-cyber-conflict/;"Israeli footprints in Iran: cyberattacks, targeted killings, more", 26 April 2021, available at: https://www.aa.com.tr/en/middle-east/israeli-footprints-in-iran-cyberattacks-targeted-killings-more/2220652.

[559] "Israel-Iran Cyber War, Gas Station Attack", 2 November 2021, available at: https://iranprimer.usip.org/blog/2021/nov/02/israel-iran-cyber-war-gas-station-attack#:~:text=Iran%20blamed%20Israel%20and%20the,fuel%20at%20a%20subsidized%20price.

[560] "Iran attacks Israel in cybersphere 'daily' Netanyahu charges", 29 January 2019, available at: https://www.timesofisrael.com/iran-attacks-israel-in-cybersphere-daily-netanyahu-charges/.

[561] "Iran says key Natanz nuclear facility hit by 'sabotage'", 12 April 2021, available at: https://www.bbc.com/news/world-middle-east-56708778.

[562] UN OEWG 2021-2025, First Substantive Session, 13 December 2021, available at: https://dig.watch/events/un-oewg-2021-2025-1st-substantive-session/international-law; R.

of them are represented in the UN GGE. Israel officially accepts the application of the prohibition of the use of force to cyber operations with the kinetic-equivalence approach, while leaving open the possibility of non-physical operations for future consideration.[563] It remains inconclusive on the issue of sovereignty. Israel also accepts the application of IHL.[564] But it maintains that human rights obligations do not apply extraterritorially.[565] On its part, Iran recognises that sovereignty of a State may be violated by cyber operations, even without "*tangible implications*".[566] Iran has a rather broad understanding of non-intervention by cyber means, yet focused on antigovernmental coercion. Iran's definition of use of force in cyberspace resembles that of the Tallinn Manual.[567] No further official positions are available.

3.2. APPLYING THE LAW TO THE ISRAEL – IRAN CONFLICT

3.2.1. State responsibility

127. Most of the operations seem to be launched by non-State actors.[568] At least politically (but nevertheless publicly), both States link these non-State actors to the opponent State and treat the operations as those of the State. The statements are largely limited to claims of technical attribution and do not rely on the classic formulation of the legal attribution rules. There is insufficient information publicly available to determine the actual control (crucial or otherwise) exercised by the States over these non-State actors. For this reason, the paper will presume attribution for these operations.[569]

128. The situation is different for cyber operations launched by 'Mossad', the national intelligence agency of Israel. Given that it is a *de iure* organ of the State,

---

SCHÖNDORF, "Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations", *International Law Studies* 2021, Vol. 97, 395-406, 398.

[563] R. SCHÖNDORF, "Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations", *International Law Studies* 2021, Vol. 97, 395-406, 398-399.

[564] R. SCHÖNDORF, "Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations", *International Law Studies* 2021, Vol. 97, 395-406, 399.

[565] G. RONA and L. AARONS, "State Responsibility to Respect, Protect and Fulfill Human Rights Obligations in Cyberspace", *Journal of National Security Law and Policy* 2016, Vol. 8, 503-530; ICJ, Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory opinion, *I.C.J. Rep.* 2004, paragraphs 109-111.

[566] Declaration of General Staff of the Armed Forces of the Islamic Republic of Iran Regarding International Law Applicable to the Cyberspace, August 2020, available at: https://nournews.ir/En/News/53144/General-Staff-of-Iranian-Armed-Forces-Warns-of-Tough-Reaction-to-Any-Cyber-Threat.

[567] Declaration of General Staff of the Armed Forces of the Islamic Republic of Iran Regarding International Law Applicable to the Cyberspace, August 2020, available at: https://nournews.ir/En/News/53144/General-Staff-of-Iranian-Armed-Forces-Warns-of-Tough-Reaction-to-Any-Cyber-Threat.

[568] "Israel-Iran Cyber War, Gas Station Attack", 2 November 2021, available at: https://iranprimer.usip.org/blog/2021/nov/02/israel-iran-cyber-war-gas-station-attack#:~:text=Iran%20blamed%20Israel%20and%20the,fuel%20at%20a%20subsidized%20price.

[569] Belfer Center Special Report, *Deterring Terror – How Israel Confronts the Next Generation of Threats (English Translation of the Official Strategy of the Israel Defense Forces*, 2016, 48.

its operations are attributable to Israel per article 4 ARSIWA. The same is true for operations launched by the Iranian 'Ministry of Intelligence'. Interestingly, for the latest cyber operation against the Natanz nuclear facility, Israeli public media claimed involvement of Mossad, which was not disputed by officials like earlier claims.[570] The public statements from Israeli officials referring to the incident do not deny any involvement and, contrary to the initial circumstantial evidence for Stuxnet,[571] may amount to acknowledgement or adoption (*supra*, p. 27).[572]

129. Perhaps because they treat the operations as those of the State, neither State has invoked a due diligence obligation on part of the other State to prevent such operations – though both States are not keen on a binding due diligence obligation either.[573] Finally, it must be reminded that, in the absence of attribution, certain acts of support can amount to non-intervention or the use of by the State (*supra*, p. 21).[574]

3.2.2. Qualifying the operations

130. Except for Stuxnet, the operations did not cause physical damage. While essentially it is sabotage,[575] the Stuxnet attack against Iran is generally accepted as meeting the use of force threshold because of its significant physical destructive effects: around 1.000 centrifuges were destroyed.[576] It is argued that it constituted 'armed force', triggering an international armed conflict.[577]

131. Because of its intention to coerce Iran to change its domestic nuclear policy, Stuxnet also clearly constituted a prohibited intervention.[578] The same is

---

[570] "Israel appears to confirm it carried out cyberattack on Iran nuclear facility", 11 April 2021, available at: https://www.theguardian.com/world/2021/apr/11/israel-appears-confirm-cyberattack-iran-nuclear-facility.

[571] F. DELERUE, *Cyber Operations and International Law*, Cambridge, Cambridge University Press, 2020, 155.

[572] "Israel appears to confirm it carried out cyberattack on Iran nuclear facility", 11 April 2021, available at: https://www.theguardian.com/world/2021/apr/11/israel-appears-confirm-cyberattack-iran-nuclear-facility.

[573] R. SCHÖNDORF, "Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations", *International Law Studies* 2021, Vol. 97, 395-406, 404; UN OEWG 2021-2025, First Substantive Session, 13 December 2021, available at: https://dig.watch/events/un-oewg-2021-2025-1st-substantive-session/international-law.

[574] ICJ, Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Judgment, *I.C.J. Reports* 1986, paragraph 228.

[575] T. D. GILL, "International humanitarian law applied to cyber-warfare: precautions, proportionality and the notion of 'attack' under the humanitarian law of armed conflict" in N. TSAGOURIAS and R. BUCHAN (eds.), *Research Handbook on International Law and Cyberspace*, Cheltenham, Edward Elgar Publishing, 2015, 366-379, 370.

[576] G. BROWN, "Why Iran didn't admit Stuxnet was an attack" *Joint Force Quarterly* 2011, 63(4), 71; F. DELERUE, *Cyber Operations and International Law*, Cambridge, Cambridge University Press, 2020, 310; Tallinn Manual 2.0, 342.

[577] M. N. SCHMITT, "Classification of Cyber Conflict", *Journal of Conflict and Security Law* 2012, Vol.17(2), 245-260, 251-252.

[578] F. DELERUE, *Cyber Operations and International Law*, Cambridge, Cambridge University Press, 2020, 241; S. J. SHACKELFORD, S. RUSSEL and A. KUEHN, "Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors", *Chicago Journal of International Law* 2016, Vol. 17(1), 13.

true for the 2021 cyber operation causing a large-scale blackout at the Natanz nuclear facility by damaging the electricity grid.[579] And despite the Iranian president describing the attack on Iranian fuel supplies as "*an attempt to annoy citizens*" (but at the same time speaking of "*cyber terrorism*"),[580] this author argues that it may very well qualify as a prohibited intervention. Concretely, the operation disabled a system that allows Iranian citizens to buy fuel at a subsidized price.[581] The timing, exactly two years after the bloody political protests that swept Iran due to the sharp rise of fuel prices at the time, is also relevant.[582] Furthermore, digital billboards were simultaneously defaced to display anti-governmental messages.[583] For these reasons, the total operation may be seen as "*instigating acts of civil strife*" and therefore be coercive.[584] Unless one argues that the strategy of both States with all their operations is to destabilise the other State by creating civil unrest,[585] the other operations lack coercion.

132. Qualifying the Israeli water filtering systems incident is challenging. Water facilities undoubtedly qualify as critical infrastructure,[586] but under *lex lata* this does not immediately seem to influence the qualification of the operation. If the tampering with chlorine levels would have been successful, it would have had to had at least amounted to injury of persons for a qualification as a use of force.[587] In other circumstances, even if tens of thousands of civilians would be left without drinkable water, there seems to be no internationally wrongful act committed. In circumstances such as these, proposals to include "(*significant*) *disruption of essential services*" seem desirable (*supra*, p. 39, 44).[588] Logic would

---

[579] "Israel appears to confirm it carried out cyberattack on Iran nuclear facility", 11 April 2021, available at: https://www.theguardian.com/world/2021/apr/11/israel-appears-confirm-cyberattack-iran-nuclear-facility.

[580] "Iran Responds to Israeli Cyber Attack", 28 October 2021, available at: https://english.aawsat.com/home/article/3271846/iran-responds-israeli-cyber-attack.

[581] "Israel-Iran Cyber War, Gas Station Attack", 2 November 2021, available at: https://iranprimer.usip.org/blog/2021/nov/02/israel-iran-cyber-war-gas-station-attack#:~:text=Iran%20blamed%20Israel%20and%20the,fuel%20at%20a%20subsidized%20price.

[582] "Iran Responds to Israeli Cyber Attack", 28 October 2021, available at: https://english.aawsat.com/home/article/3271846/iran-responds-israeli-cyber-attack.

[583] "Israel-Iran Cyber War, Gas Station Attack", 2 November 2021, available at: https://iranprimer.usip.org/blog/2021/nov/02/israel-iran-cyber-war-gas-station-attack#:~:text=Iran%20blamed%20Israel%20and%20the,fuel%20at%20a%20subsidized%20price.

[584] Resolution of the UN General Assembly, Declaration on Principles of International law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations (24 Oct 1970). *UN.Doc.* A/RES/25/2625, Principle 1.

[585] "A hacking slugfest between Iran and its foes sparks fears of a wider cyberwar", 23 December 2021, available at: https://www.latimes.com/world-nation/story/2021-12-23/iran-israel-hacking-heightens-fears-cyberwar.

[586] N. TSAGOURIAS, "Cyberattacks, self-defence and the problem of attribution", *Journal of Conflict & Security Law* 17(2), 229-244, 231.

[587] The failure or prevention of an operation renders it no longer a violation of sovereignty, see: Tallinn Manual 2.0, 24 and 419.

[588] M. ROSCINI, "Cyber operations as a use of force" in N. TSAGOURIAS and R. BUCHAN (eds.), *Research Handbook on International Law and Cyberspace*, Cheltenham, Edward Elgar Publishing, 2015, 233-254, 253; N. TSAGOURIAS, "Cyberattacks, self-defence and the problem of attribution", *Journal of Conflict & Security Law* 17(2), 229-244, 231; E. T. JENSEN, "Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defence" *Standford Journal of International Law* 38, 221-229.

also suggest that under a consequence-based approach, States will regard such an operation, if successful, as a use of force.[589]

133. The cyber operation targeting the computer systems that regulated the flow of vessels, trucks and goods within the Shahid Rajaee port is a prime example of "*the remote causation of loss of functionality of cyber infrastructure located in another State*", the legal status of which is unsettled according to the Tallinn Manual.[590] Although maritime traffic was severely disrupted for multiple days, causing massive economic and reputational damage, no incidents of physical damage were reported. There is no information on what was necessary to restore the functionality. With no coercive element, the incident seems to escape any qualification as an internationally wrongful act.

134. Finally, deciding on whether there has been a violation of sovereignty is the most difficult and controversial exercise. Absent any physical manifestations (whatever threshold one agrees upon), a qualification as a violation of sovereignty is unlikely under *lex lata*. Serving as a useful illustration, while the 2021 sabotage of the Natanz facility with smuggled-in explosives most probably violates Iran's sovereignty, the cyber equivalent probably does not.[591] Under the strict inviolability approach or under a consequence-based approach, all operations but the data leaks could qualify as violations of sovereignty.

3.2.3. The law of cyber armed conflict

135. The law of armed conflict applies if one accepts that one of the cyber operations amounted to armed force, which is argued in relation to Stuxnet.[592] Even so, given that isolated incidents are rarely considered triggering IHL,[593] it seems unlikely that Stuxnet can be seen as the starting point of an on-going international armed conflict. The other option is that the (mostly indirect) physical face-offs between the two States have created an international armed conflict between them, and that therefore the parallel cyber operations are regulated by IHL. Although there is no general claim as to the applicability of IHL by either State, an Israeli official did state that the Iranian operation against

---

[589] See for example the U.K.'s claim in relation to the poisoning of Mr. Sergei Skripal, stating that it was a use of force by the Russian Federation against the United Kingdom. For an analyses, see: M. WELLER, "An International Use of Force in Salisbury?", *EJIL:Talk!*, 14 March 2018, available at: https://www.ejiltalk.org/an-international-use-of-force-in-salisbury/.

[590] "Iran-Israel: the larger implications of cyber conflict", 19 September 2020, available at: https://www.strikesource.com/2020/09/19/iran-israel-the-larger-implications-of-cyber-conflict/; Tallinn Manual 2.0, 20.

[591] "Blackout Hits Iran Nuclear Site in What Appears to be Israeli Sabotage", 11 April 2021, available at: https://www.nytimes.com/2021/04/11/world/middleeast/iran-nuclear-natanz.html; "Iran Natanz nuclear site suffered major damage, official says", 13 April 2021, available at: https://www.bbc.com/news/world-middle-east-56734657.

[592] M. N. SCHMITT, "Classification of Cyber Conflict", *Journal of Conflict and Security Law* 2012, Vol.17(2), 245-260, 251-252.

[593] S. VERHOEVEN, "International and Non-International Armed Conflicts" in J. WOUTERS, P. DE MAN and N. VERLINDEN (eds.), *Armed Conflicts and the Law*, Mortsel, Intersentia, 2016, 151-186, 158.

Israeli water facilities "*is an attack that goes against all the codes of war*".[594] Therefore, for the sake of the research, let us assume that there is an international armed conflict and that IHL applies. It must be highlighted that neither State is party to AP I. Consequently, they are only bound by IHL rules that reflect customary international law, which is generally the case for the IHL principles analysed in this paper.[595]

136. Two preliminary statements can be made because they do not require an 'attack'. First, per article 54(2) AP I, rendering useless a civilian water facility is prohibited, making Iran's operation a violation of IHL because it cannot be justified under the article. Second, the article 57(1) AP I 'constant care' obligation would in any case be violated by the operations directly and carelessly targeting civilians and civilian objects (the port, the fuel stations, the hospitals, the water facility).

137. Under a kinetic effect equivalency approach, few operations would qualify as IHL attacks.[596] Otherwise, it can be argued that targeting a nuclear facility, a hospital and a water facility is always reasonably expected to cause physical damage or injury.[597] Here, distinction, proportionality and precaution apply. Israel has objected to data qualifying as objects, yet clarified that an attack targeting data is nevertheless subject to the targeting rules if it is reasonably expected to cause physical damage or injury.[598] The nuclear facility is a traditional dual-use object and can be lawfully targeted if proportionality and precautionary measures have been taken, subject to article 56 AP I on the release of dangerous forces. Finally, the Stuxnet attack is an example that arguably is prohibited under article 51(4)(c) AP I because it employed a "*method or means of combat the effects of which cannot be limited (...) and consequently (...) are of a nature to strike military objectives and civilians or civilian objects without distinction*". Indeed, even though the worm was designed for the nuclear centrifuges, afterwards it leaked throughout civilian cyber infrastructures.[599]

---

[594] "Israel aghast at Iran cyberattack on civilian water infrastructure – TV report", 9 May 2020, available at: https://www.timesofisrael.com/israel-aghast-at-iran-cyberattack-on-civilian-water-infrastructure-tv-report/.

[595] J-M. HENCKAERTS, "Customary International Humanitarian Law: Taking Stock of the ICRC Study", *Nordic Journal of International Law* 2010, Vol. 78, 435-468, 438-439; J-M. HENCKAERTS and L. DOSWALD-BECK, *Customary International Humanitarian Law – Volume I: Rules*, Cambridge, Cambridge University Press, 2005, 3-74, 127-138, 244-250.

[596] There is little doubt, however, that if a water facility, a nuclear facility, an international port or 4.000 fuel stations were targeted by kinetic means, causing these exact consequences, they would amount to an IHL attack; K. BANNELIER-CHRISTAKIS; "Is the principle of distinction still relevant in cyberwarfare?" in N. TSAGOURIAS and R. BUCHAN (eds.), *Research Handbook on International Law and Cyberspace*, Cheltenham, Edward Elgar Publishing, 2015, 343-365, 348.

[597] T. D. GILL, "International humanitarian law applied to cyber-warfare: precautions, proportionality and the notion of 'attack' under the humanitarian law of armed conflict" in N. TSAGOURIAS and R. BUCHAN (eds.), *Research Handbook on International Law and Cyberspace*, Cheltenham, Edward Elgar Publishing, 2015, 366-379, 376.

[598] R. SCHÖNDORF, "Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations", *International Law Studies* 2021, Vol. 97, 395-406, 401.

[599] "Whatever happened to Stuxnet", 17 January 2019, available at: https://www.synopsys.com/blogs/software-security/whatever-happened-to-stuxnet/, consulted on 30 April 2022.

3.2.4. International human rights law

138. A final issue is that of the personal data leaks. While the operations blatantly targeted civilian hospitals and sensitive civilian data, they seem to escape any qualification as international wrongful acts outside the context of an armed conflict. This means that redress for the victims can only be sought under international human rights law. Under a functional model of jurisdiction for the extraterritorial application of negative human rights obligations for States, Iran could theoretically be held responsible for these violations.[600]

4. Conclusion

139. From the perspective of State obligations, the paper has made a cross-section of various domains of international law to address some of the most important and pressing issues relating to the application of international law to cyber conflicts. First off, the paper has analysed the problem of legal attribution of cyber operations. Here, it found that the 'effective control' test is not effective in cyberspace because it stretches too far, "*almost to a breaking point*",[601] the factual reality of conducting cyber operations. Instead, the paper argues that the legal possibility exists for a specialised regime of attribution of State responsibility for cyber operations; and that this is necessary. A proposal is made for a notion of 'crucial control' or a reliance on State instruction for certain scenarios of State-backed cyber operations. Contrary to popular suggestion, the paper found that due diligence is not a suitable solution for the problem of legal attribution. After considering the different takes on due diligence, the paper came to the conclusion that a more traditional 'lightweight' variant of the due diligence obligation is most probable to be accepted by States, while still offering a solid degree of protection and responsibility.

140. Most practical problems arise in qualifying cyber operations as international wrongful acts. Categorising real-life cyber operations into existing notions of use of force, non-intervention and violation of sovereignty often feels like trying to fit a square peg into a round hole.[602] Even though a consequence-based or a 'disruption of essential services' approach might work, a dedicated Treaty on cyber safe zones would be optimal from a protective perspective.

141. The paper further found that IHL is applicable to cyber armed conflicts and dealt with the most pressing issues of applicability. Firstly, it found that cyber operations can qualify as IHL attacks. Secondly, given the interconnected nature of cyberspace, a cautious understanding of dual-use must be employed. Not *every* military use renders a civilian cyber object a lawful military target: it must still fulfil the three-step test. This also implies a meticulous proportionality

---

[600] Iran is a State party to the International Covenant on Civil and Political Rights (ICCPR) since 1975 but has never signed nor ratified the Optional Protocol I which allows for an individual complaint mechanism before the Human Rights Committee. The same is true for Israel.
[601] ICJ, *Bosnian Genocide*, paragraph 407.
[602] Or a Herman De Croo-esque alternative: it feels like forcing a kid into clothes it does not want to wear.

analysis and careful precautionary considerations. Thirdly, while the paper favours the inclusion of content-level data as objects, it suggests that content-level data is perhaps better protected under international human rights law. Concerning operational-level data, the paper favours an effects-based approach. The paper also agreed on the increased importance of certain precautionary obligations in cyber armed conflicts. Finally, when it comes to cyber conflicts and international human rights law, the paper argues for a functional model of jurisdiction for the purpose of extraterritorial application of negative human rights obligations. It also pleads that the logic against extraterritorial application during armed conflicts does not apply to situations of cyber armed conflict.

142. All in all, the challenges are diverse in nature and in scope, and may perhaps seem insurmountable. Nevertheless, this paper concludes that, except for certain proposals of progressive development, most challenges can be properly dealt with within the framework of existing international law.