Best of both worlds?
The interplay between international human rights law and the law of armed conflict in cyberspace

Tatjana Grote*

ABSTRACT

Cyberoperations are an increasingly prevalent part of armed conflict, as evidenced by the recent cyber-based incidents in Ukraine. While much has been written about how the law of armed conflict (LOAC) applies to such operations, relatively little attention has been paid to the role of international human rights law (IHRL). This article attempts to fill this gap, focusing on the law of international armed conflict. In its first part, it will be demonstrated that essential parts of LOAC are premised on the idea that only operations with violent effects like death, injury or destruction, are of a severity that would justify an obligation to distinguish between civilians and military objectives. As political, economic, and social activities move into the non-physical sphere of cyberspace, this assumption is no longer tenable. Yet, it is averred that simply applying the principle of distinction to all cyberoperations does not constitute a satisfying solution. The article hence turns to IHRL and finds that its focus on individual rights and accountability could compensate for LOAC’s shortcomings. However, IHRL’s protective value is greatly circumscribed by its limited extraterritorial applicability. The novel conclusion offered in the final section is that the true source of the existing gap in legal protection against military cyberoperations is the failure to acknowledge the possibility of affecting the enjoyment of immaterial goods and freedoms without having physical control over a person. This makes the norms of LOAC inadequate and IHRL inapplicable, leaving civilians in situations of armed conflict vulnerable to severely harmful cyberoperations.

*LLM (LSE) ‘22, Carlo-Schmid Fellow at the International Criminal Court (ICC). The views expressed by the author in this article are their own and do not represent the views of the ICC.
INTRODUCTION

Recent cyberoperations against government websites and private companies in Ukraine have once again shown that cyberspace plays an important role in modern armed conflict.¹ Long before Russia’s invasion of Ukraine, military cyberoperations have been a cause of concern, *inter alia*, for the legal protection of civilians from the effects of armed conflict. Although there now seems to be widespread consensus that the law of armed conflict (LOAC) generally applies to cyberoperations with a nexus to armed conflict,² many commentators lament a lack of protection against one specific type of operation: cyberoperations without any reasonably foreseeable physical effects.³ This category could include operations deleting civilian banking data, disabling navigation systems or blocking access to messaging services.


³ Cyberoperations can have complex indirect effects. While there is no absolute clarity as to if and to what extent these effects need to be taken into account, this work will adopt the majority approach of the Tallinn Manual and consider a cyberoperations as devoid of physical effects if no physical effects were intended or reasonably foreseeable. NATO Cooperative Cyber Defence Centre of Excellence (n 2) 416, para. 5.
Traditionally, a crucial avenue for providing protection has been the principle of distinction, which obliges belligerent parties to distinguish between civilians and civilian objects on the one hand, and combatants as well as military objectives on the other. Only the latter two categories constitute legitimate targets. The most important provisions operationalising the cardinal principle of distinction are predominantly framed with reference to ‘attacks’ and ‘objects’. Since these terms have traditionally been interpreted to require physicality in the effects and targets of an operation, many hold that if an operation does not produce physical effects or damage to tangible objects, it does not qualify as an ‘attack’ (defined in Article 49(1) Additional Protocol 1, AP1). Accordingly, there would be no general requirement to limit such operations to military objectives. Many conclude that this causes a lack of legal protection from severely harmful, non-physical effects of cyberoperations. While much has been written on whether and to what extent this focus on physical effects and objects limits the applicability of the principle of distinction, this paper will take a step back and challenge a recurring, underlying assumption of these debates: that the current gap in legal protection of civilians from harmful cyberoperations without physical effects is caused by the aforementioned focus on physicality (‘physical anchoring’) of LOAC.

4 See Article 48 Additional Protocol (AP) 1.
6 As will be discussed below, the ICRC commentary as well as many scholars consider ‘tangibility’ an inherent characteristic of any ‘object’.
7 The phrase ‘cyber-contained’ will be used to denote cyberoperations without any reasonably foreseeable physical effects.
8 This perspective is especially relevant with a view to the hybrid model of warfare, which combines conventional methods of warfare with disinformation operations and economic measures. In times where what is traditionally understood as violence – physical force – is combined with other types of force, clarifying which norms of international law are applicable to which subsets of operations forming part of this form of warfare is crucial. On hybrid warfare, see Arsalan Bilal, ‘NATO Review – Hybrid Warfare – New Threats, Complexity, and “Trust” as the Antidote’ (NATO Review, 30 November 2021) <https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html> accessed 16 February 2023.
In doing so, this paper will only examine cyberoperations with a nexus to armed conflict, i.e., operations to which LOAC is generally applicable. Such operations are considered most likely to be conducted by states in support of kinetic operations in an international armed conflict (IAC). Furthermore, it should be noted that operations with a substantive impact on the civilian population are often traced back to state-led cyber commands as they require a high level of technical expertise and resources, which many non-state actors lack. Therefore, the following analysis will focus on the law of IAC from a state actor perspective. While the issue of attribution (i.e., legally connecting the actions of private persons to a state) is highly relevant, it is less crucial for this work since it is not focused on ensuring accountability, but on the rules limiting states’ conduct in cyberspace in the first place. Moreover, attribution is usually less problematic if an operation is linked to ongoing, kinetic hostilities. This was illustrated by the attribution of a cyberoperation by, inter alia, the European Union, to Russia at the dawn of its invasion of Ukraine.

---

10 See Tallinn Manual (n 2), Rule 80; NATO Cooperative Cyber Defence Centre of Excellence (n 2) 376, para. 5.
11 Kinetic operations are understood as operations relying on the motion of physical material bodies and the associated release of energy to create physical effects. An example of such an operation would be the destruction of a bridge using a bomb. Terry D Gill, ‘International Humanitarian Law Applied to Cyber-Warfare: Precautions, Proportionality and the Notion of “Attack” under the Humanitarian Law of Armed Conflict’ in Nicholas Tsagourias and Russell Buchan (eds), Research Handbook on International Law and Cyberspace (Edward Elgar Publishing 2021) 458; ibid 469; ‘Definition of Kinetic’ (Merriam-Webster, 30 December 2022) <https://www.merriam-webster.com/dictionary/kinetic> accessed 16 February 2023.
14 James Gow, ‘The Ambiguities of Cyber Security’ in James Gow and others (eds), Routledge Handbook of War, Law and Technology(1st cdn, Routledge 2019) 120.
The following section will give an overview of military cyberoperations and the existing LOAC literature thereon. Section Three will then argue that, even if applicable, it seems unlikely that the principle of distinction can provide meaningful protection against non-physical harm as the interconnected and complex nature of cyberspace make both the distinction and assessment of proportionality an overwhelmingly difficult exercise. Section Four will then illustrate why international human rights law (IHRL) might be more apt to regulate cyberoperations meaningfully due to its focus on transparency, accountability and individual rights. However, a crucial shortcoming of the protection provided by IHRL remains its limited extraterritorial applicability. Taking both sections together, it is concluded that the current gap in legal protection arises from more than just the non-violent nature of certain cyberoperations. Both LOAC and IHRL provide protection against non-physical harm, but only for persons in the hands of, or under the effective control of, a state. Hence, the current lack of protection is not solely attributable to LOAC’s focus on physical effects and objects, but rather to the possibility of directly targeting immaterial goods and values without having physical control over the persons who will feel the consequences of such operations.

I. ‘UPDATE REQUIRED’? WHY SOME MILITARY CYBEROPERATIONS MIGHT NOT BE COVERED BY THE PRINCIPLE OF DISTINCTION

Cyberoperations have been defined by the International Committee of the Red Cross (ICRC) as ‘operations against a computer, a computer system or network, or another connected device, through a data stream’.¹⁶ Operations forming part of this category can produce idiosyncratic effects on a great variety of targets. Due to this peculiarity, it is crucial to differentiate between different types of operations as some are accepted to be covered by existing law, whereas others are considered to fall between the gaps of the current LOAC. This section will describe some of the most notable cyber-incidents and elaborate on

why some of these operations might elude the current protections under LOAC. In discussing how commentators propose to address the identified gap in legal protection, it will be argued that the existing proposals remain vague and overall unconvincing.

A preliminary note on the scope of the following analysis is warranted. As mentioned above, this article focuses on the law of international armed conflict from a state actor perspective. This focus has been chosen for the following reasons. Many of the most consequential operations have been tentatively linked to state actors.\(^\text{17}\) This must not be confused with a legal attribution of such operations to a state. Yet, it shows that despite the certainly crucial role of non-state actors in cyberspace, state actors are still at least as relevant. In fact, as states have ‘inexhaustible resources, an educated and trained workforce of cyber-attackers, and military and economic motivations’,\(^\text{18}\) it might generally be more likely that large-scale operations with a significant impact on the civilian population are conducted by states rather than non-state actors.\(^\text{19}\) Especially in armed conflict, where quick and precise action is essential, it seems unlikely that the many states which have established military cyber commands over the past years\(^\text{20}\) would completely outsource the most impactful (and hence sophisticated) operations to non-state groups. While questions of attribution and the obligations of non-state actors remain highly relevant, they are beyond the remit of this work since the focus here is on the obligations to which states have to adhere when conducting cyberoperations. This is not to say that holding states accountable for their cyberoperations, which requires attribution, is not pivotal. Rather, this article deliberately focuses on the question preceding attribution for the purpose of holding states accountable with respect to their obligations under international law, namely: what are these obligations?

\(^{17}\) Most notably Stuxnet and the recent Ukraine satellite internet incident, which will be explored below.

\(^{18}\) Stiennon (n 12) 14.

\(^{19}\) Gill (n 11) 427.

\(^{20}\) Stiennon (n 12) 25–27.
1.1 Existing protections: which cyberoperations are covered by the law of targeting as it stands?

When cyberoperations have reasonably foreseeable physical effects, the law of targeting (i.e., those norms regulating which persons and objects can lawfully be targeted in armed conflict) applies as usual. There is widespread agreement that an operation with a nexus to armed conflict intended to physically damage, kill or cause injury can be considered an ‘attack’. Note that the reference to ‘violence’ in Article 49(1) AP1 does not relate to the means of creating certain effects, but the effects as such.\(^\text{21}\) Hence, if violent effects (including serious mental injury)\(^\text{22}\) are created through non-violent cyberoperations, they nevertheless qualify as attacks. One example of such an operation is the malware *Stuxnet*, which significantly damaged turbines in the Iranian nuclear facility Natanz, thus delaying Iran’s nuclear program by roughly two years.\(^\text{23}\) The operation was significant because it was one of the few operations to this date that employed cyber-means to produce physical damage,\(^\text{24}\) and which could hence be qualified as an attack within the meaning of Article 49(1) AP1.

However, modern reliance on cyberspace introduces a critical new harm vector: by targeting sensitive data or rendering crucial cyber-based services dysfunctional or inaccessible, severe harm can be caused, even in absence of physical effects. This was shown by several ransomware operations affecting health facilities, *inter alia*, in the UK.\(^\text{25}\) Yet, granted a nexus with armed conflict exists, such operations are covered by extant LOAC since certain targets like

\(^{21}\) NATO Cooperative Cyber Defence Centre of Excellence (n 2) 415.


\(^{23}\) Stiennon (n 12) 20.


health facilities,\textsuperscript{26} humanitarian relief operations,\textsuperscript{27} cultural objects and places of worship\textsuperscript{28} as well as objects indispensable to the survival of the civilian population\textsuperscript{29} are protected not only against attacks, but against ‘military operations’ or, for cultural objects and places of worship, any ‘act of hostility’.\textsuperscript{30} Nevertheless, these operations constitute only a small subset of all possible operations with severely harmful effects on civilians.

More general protection is provided by Article 57(1) AP1, which stipulates that the belligerents have to take constant care to spare the civilian population during all operations.\textsuperscript{31} However, this is a rather vague standard.\textsuperscript{32} It is only the more specific rules of the principle of distinction that allow states to be held accountable with respect to concrete obligations and prohibitions.

1.2 Gaps in protection: how to undo the physical anchoring of the principle of distinction?

While the previous subsection illustrated that certain cyberoperations are satisfyingly covered by existing law, the following section will illustrate why those operations not creating any physical effects against targets other than those enjoying special protection might escape the reach of the specific prohibitions and obligations of the principle of distinction.

\textsuperscript{26} Article 12(1) AP1.
\textsuperscript{27} Articles 70(4), 71(2) AP1.
\textsuperscript{28} Article 53(a) AP1.
\textsuperscript{29} Article 54(2) AP1.
\textsuperscript{30} This does not mean that this protection is absolute. In fact, the protection of cultural property and objects indispensable to the survival of the civilian population are caveatd by exceptions based on the concept of military necessity (see Article 4(2) Hague Convention for the Protection of Cultural Property, Article 56(5) AP1). Gisel, Rodenhäuser and Dörmann (n 13) 327–329.
\textsuperscript{32} This standard is less strong than the more specific rules in Articles 51-56 AP1 since it does not constitute a prohibition on targeting certain objects or persons. Instead of defining explicitly what belligerent parties must or must not do, Article 57(1) AP1 leaves it to commanders to define which steps are necessary and feasible to take constant care. Concrete duties are only spelled out in the subsequent paragraphs, which refer to ‘attacks’, not military operations. Overall, Article 57(1) has been compared to Article 48 AP1, since both contain general principles which are only clarified by other provisions.
The principle of distinction is formulated in general terms in Article 48 AP1 with reference to all ‘military operations’:

In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives.

However, provisions operationalising the principle only mention ‘attacks’. Therefore, the interpretation of its definition (‘acts of violence’, Article 49(1) AP1) has been considered crucially important. Some commentators propose a *strict physical effects approach* according to which only a cyberoperation intentionally or reasonably foreseeably causing violent effects in a traditional sense, i.e., physical effects, would qualify as an attack. While this approach stays true to the ordinary meaning of the term ‘violence’ at the time when the drafters chose this term, it leads to absurd results: the physical destruction of a server hosting a critical civilian service would be unlawful while rendering it dysfunctional through cyber-means (e.g., like the cyberoperations against Ukraine in 2022) would be lawful despite producing the same effect on civilians. Apart from this conceptually unsatisfying outcome, following the strict physical effects approach would substantially limit the legal protection against cyberoperations provided by the principle of distinction, potentially leading to a situation where an operation severely harming civilians would be perfectly lawful under LOAC.

---

33 See, e.g., Article 51(2), (4), (5), (6); Article 52(2), Article 55(2), Article 56(1), Article 57(2) AP1.
The consequences of adopting a *strict physical effects approach* are of great relevance in light of past cyberoperations. In 2007, Estonia became the target of one of the first large-scale cyberoperations. In reaction to the removal of a Soviet statue, Estonian banking, telecommunications and government websites were flooded with requests from hijacked computers,\(^{38}\) causing many services to be unavailable for some time. One year later, Georgia became the target of similar operations which were considered to be linked with the Russian use of force in the same year.\(^{39}\) First, hijacked computers overwhelmed government-related cyber-services, including the Social Assistance and Employment State agency, with fake requests thus causing them to break down.\(^{40}\) Then, on the eve of the Russian invasion of Georgia, essential cyber-based communication systems were disabled, effectively isolating the country and its citizens from their government and the rest of the world.\(^{41}\)

More recently, military cyberoperations were employed in connection with the armed conflict in Ukraine. On the eve of the Russian invasion in 2022, a cyberoperation rendered thousands of satellite internet modems dysfunctional, ‘causing indiscriminate communication outages and disruptions across several public authorities, businesses and [private] users in Ukraine’.\(^{42}\) Furthermore, multiple distributed denial-of-service (DDoS) operations crippled the websites of several Ukrainian banks and government agencies.\(^{43}\)

All three examples highlight that cyberoperations can cause highly disruptive, and yet entirely non-physical, effects. If the principle of distinction does not apply in such operations, civilians might lawfully be subjected to such

---

\(^{38}\) Stiennon (n 12) 17. This type of operation is called Distributed-Denial-of-Service (DDoS) operation and is one of the less sophisticated but common ways to render services dysfunctional; UK National Cybersecurity Centre, ‘Denial of Service (DoS) Guidance’ (<https://www.ncsc.gov.uk/collection/denial-service-dos-guidance-collection> accessed 16 February 2023).

\(^{39}\) Stiennon (n 12) 20.

\(^{40}\) ibid 18.

\(^{41}\) ibid 19.

\(^{42}\) Council of the EU (n 15).

effects under IHL. In light of this, three avenues have been explored to undo this ‘physical anchoring’ of the principle of distinction.

2.2.1 Option 1: The principle of distinction applies to all military operations

Some commentators contend that the principle of distinction applies not only to attacks, but to military operations more broadly. According to one commentator, the principles of distinction, proportionality and precaution, ‘accurately understood’, apply to hostilities, i.e., all operations that are meant to harm the adversary through physical effects or other means. Based on a systematic interpretation of AP1, another commentator avers that if the principles of distinction, proportionality and precaution only applied to attacks, Article 48 AP1 in general, and the chapeaux of Article 51 and Article 57 AP1, would be superfluous.

These views, however, are unconvincing. In fact, it is hard to deny that the more specific norms of LOAC, which are considered to give effect to the principle of distinction, explicitly refer to attacks. During the negotiations of AP1, the delegation of the UK, in fact, pointed out that the broadly framed basic rule in Article 48 AP1 was meant as a general rule and commanders would rather consult Article 52 AP1, which contains a specific prohibition on targeting civilian objects and a definition thereof, when making targeting decisions. The
delegation of Israel explicitly stated that the reference to ‘military operations’ in Article 51(1) AP1 should not be seen as a derogation from the narrower protection of the civilian population against attacks only, and suggested the term (‘attack’) instead to avoid inconsistencies.\textsuperscript{49} These statements are hard to ignore, especially because they are in line with current state practice.\textsuperscript{50}

In light of the foregoing, this author believes that the use of the term ‘military operations’ in the \textit{chapeaux} of Articles 51 and 57 as well as Article 48 AP1 does not allow for the conclusion that specific rules which solely mention the term ‘attack’ are applicable to all ‘military operations’. Indeed, it would be hard to explain why the drafters felt the need to legally define ‘attacks’ instead of ‘military operations’, if all the provisions using this term were applicable to the latter category instead of the former. Instead, Articles 51 and 57 as well as Article 48 AP1 should be considered introductory, preamble-like provisions, which formulate the general principle underlying the subsequent rules without altering the content of these more specific norms.

Moreover, the precise definitions of ‘hostilities’ and ‘military operations’ remain unclear. The first is notoriously controversial\textsuperscript{51} and the latter is defined in two different ways by the ICRC commentary to AP1.\textsuperscript{52} Hence, even if the principles of distinction, proportionality and precaution did apply to all military operations or hostilities, there is still a need to delimit these two categories from another category of military activity which can lawfully be directed at civilians. Such a category undoubtedly exists given that espionage and

\textsuperscript{49} ibid 223, paras 36-37.
\textsuperscript{50} Schmitt (n 47) 7.
\textsuperscript{51} The notion of ‘hostilities’ has been relevant in the context of defining the phrase ‘direct participation in hostilities’. This phrase is of utmost important as civilians directly participating in hostilities can be targeted lawfully (see Article 51(3) AP1, Article 13(3) Additional Protocol 2); Nils Melzer and International Committee of the Red Cross, \textit{Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law} (International Committee of the Red Cross 2009) 43.
psychological operations are widely accepted as lawful, even where conducted indiscriminately.  

2.2.2 Option 2: Re-interpreting the term ‘violence’

Another avenue for making all rules of targeting applicable to cyberoperations without physical effects is to reinterpret the meaning of ‘violence’ in Article 49(1) AP1. The experts of the Tallinn Manual (TM) introduced the functionality approach by defining a cyberattack as ‘a cyber operation … that is reasonably expected to cause injury or death to persons or damage or destruction to objects’. At first sight, the definition does not seem to deviate from a strict physical effects approach. The key innovation is hidden in the TM majority’s conclusion that a mere loss of functionality could qualify as ‘damage’. However, most experts held that this was only the case if the restoration of functionality would require the replacement of a physical component. This reading hence maintains the requirement of physical effects but covers even de minimis damage, where it renders a system dysfunctional. This insistence on some kind of physical effect is in line with the legal positions expressed in statements of several states, for example Peru and Denmark, on the application of LOAC to cyberoperations.

Only few TM experts contend that a mere loss of functionality, regardless of which type of action is required to render the targeted system or device functional again, would amount to ‘damage’ within the meaning of AP1. This view, however, has been prominently expressed outside the TM process. One commentator points to the mention of ‘neutralisation’ in Article 52(2) AP1 to suggest that the drafters did not consider the notion of attacks to be strictly limited to violent operations, but meant to also include operations

54 The Tallinn Manual is an academic publication on the international law applicable to cyber warfare. It is the outcome of discussions between roughly twenty experts of international law. Despite not being binding, it is one of the most commonly referenced and comprehensive publications on international law and military cyberoperations.
55 NATO Cooperative Cyber Defence Centre of Excellence (n 2) 415.
56 The TM experts held that, otherwise, de minimis damage would not be included. ibid 416.
57 Gisel, Rodenhäuser and Dörmann (n 13) 314.
58 NATO Cooperative Cyber Defence Centre of Excellence (n 2) 418.
affecting the functionality of a military objective. The ICRC recently confirmed its view that ‘during an armed conflict an operation designed to disable a computer or a computer network constitutes an attack under [LOAC]’, regardless of how the system is disabled. Such a strict functionality-based approach has been adopted by France.

Another commentator suggests that if the effects of a cyberoperation exceed merely transient inconveniences and ‘cause significant functional harm to infrastructures’, they should be considered ‘attacks’. Such a focus on critical infrastructure was also reflected in the positions of Bolivia, Ecuador and Guyana. Germany takes a very broad effects-based approach, stating that any ‘harmful effects’ on cyber systems or data amount to an attack. The criterion of permanency was emphasised by another author. One commentator suggested that a cyberoperation amounts to an attack if the effects it produces would be considered ‘damage’ if they were the result of a kinetic operation. Both Australia and the UK subscribe to this idea.

It is therefore clear that there are varied views on whether and how to reinterpret violence. Some commentators focus on the functionality of a system,

60 International Committee of the Red Cross (n 16) 488–489.
61 Gisel, Rodenhäuser and Dörmann (n 13) 315–316.
62 Marco Roscini, ‘Proportionality in Cyber Targeting’ in James Gow and others (eds), Routledge Handbook of War, Law and Technology (Routledge 2019) 90.
63 Gisel, Rodenhäuser and Dörmann (n 13) 316.
65 Gill (n 11) 467.
66 Jensen (n 31) 205–206.
others on the severity and permanency of the effects of an operation for civilians, others on an equivalency with the effects of a kinetic attack. All these approaches share one problematic feature. If physical effects are discarded as a threshold, there is a need to create a straightforward alternative test to identify situations in which the harm to civilians emanating from an operation is so great that a distinction is necessary. Only few would dispute that such a threshold exists as espionage and psychological operations are traditionally not considered to be covered by the principle of distinction. Even the ICRC stated that civilians are not protected from certain inconveniences caused by armed conflict.

The strict functionality approach sets out a clear threshold, namely at the level where the functionality of a system is impacted. This assumes that there is a strong and consistent correlation between severely harmful effects on civilians and a loss of functionality. However, this assumption might not hold for all systems. For instance, if a belligerent party were to disable a streaming platform, this would arguably not amount to an operation from which civilians need to be shielded. It thus seems reasonable to refer to the severity of the effects of an operation on the civilian population. The above discussion showed that some authors have proposed effects which exceed ‘merely transient inconveniences’ as a new threshold. Yet, the term ‘inconveniences’ seems unhelpful as it is not mentioned in LOAC treaties, and is hence not defined. Equally, the notion of ‘effects equivalent to those of a kinetic attack’ would require further clarification to provide meaningful guidance. Another approach that has been proposed is to accord protection to ‘essential civilian functions or

68 Note that one crucial question of all approaches focusing on the effects of an operation is which effects are considered as directly attributable to a specific operation. For instance, an operation leaking sensitive data of certain vulnerable individuals might lead to these persons being harmed. The Tallinn Manual experts held that only if such indirect effects are reasonably foreseeable or intended do they need to be taken into account. This standard seems widely accepted and has not been the subject of much academic discussion. However, the question of how to legally classify indirect effects of cyberoperations should be kept in mind as one that could potentially bring many operations within the scope of the traditional definition of ‘attacks’; NATO Cooperative Cyber Defence Centre of Excellence (n 2) 416, para. 5.


70 Schmitt, ‘Wired Warfare 3.0’ (n 53) 339.

71 Bannelier (n 2) 441.
services’, instead of all types of services and data. However, this would require consensus as to which parts of the ICT infrastructure, and which online services and types of data are essential. While there might be a core set of services and infrastructure commonly accepted as essential, disagreement about the precise extent of this category seems highly likely.\(^{72}\)

Consequently, while there are many general ideas on how to re-interpret violence, the devil seems to lie in the details of proposing a stringent and clear alternative threshold for making the principle of distinction applicable. As will be proposed below, there might be merit in the idea of discarding an exclusive focus on LOAC in this respect, and instead consider the human rights guarantees and the relevant jurisprudence thereon when assessing which type and degree of harm civilians must not be subjected to.

### 2.2.3 Option 3: Data as an object

Another way to bring certain cyberoperations without physical effects under the protective umbrella of the principle of distinction would be to interpret data as an object within the meaning of Article 52(1) AP1, which states that ‘[c]ivilian objects shall not be the object of attack or of reprisals.’ Civilian objects are negatively defined as all objects which do not constitute military objectives as defined in Article 52(2) AP1, i.e., ‘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’. While Article 52(1) AP1 also mentions ‘attacks’, it has been argued that if data was considered an object, its deletion would then clearly constitute damage, and the operation hence an attack.\(^{73}\) While the TM majority rejected this approach with a view to the ordinary meaning of the term ‘object’ and its definition in the ICRC Commentary to AP1 as ‘something that is visible and tangible’,\(^{74}\) one commentator suggested that this ‘ordinary meaning’ is not as clear as the TM experts suggested.\(^{75}\) Another commentator distinguished between content level data (digital information understandable by humans) and operational level data

\(^{72}\) Schmitt, ‘Wired Warfare 3.0’ (n 53) 346–347.

\(^{73}\) ibid 340.

\(^{74}\) Pilloud and others (n 52), para 2008.

\(^{75}\) Mačák (n 35) 59.
(code determining the functioning of cyber-systems) and claimed the latter could be a military objective.\textsuperscript{76} These approaches are increasingly adopted by states: Finland, Germany, Romania and Norway now hold that civilian data is protected as a civilian object.\textsuperscript{77} France considers civilian content level data protected.\textsuperscript{78}

There is some intuitive appeal in both approaches as they would allow for the extension of protection of civilian objects to civilian data. However, two problems emerge.

First, interpreting data as an object alone will not protect civilians from all potentially harmful operations. Imagine a DDoS operation on the banking sector that makes monetary withdrawals impossible. Denial of Service (DoS) operations render systems dysfunctional without destroying data or altering code in any way. Instead, they overflood a system with requests, causing it to break down.\textsuperscript{79} Accordingly, this type of operation can create severe consequences without deleting or tampering with any data.\textsuperscript{80} Prohibiting the deletion of civilian data alone thus would not provide protection against the effects of DDoS or similar operations.

Second, granting the same protection to all civilian data might be overinclusive. Arguing that there is a need to extend the general legal protection provided by the principle of distinction to civilian objects to all types of data relies on the assumption that the deletion or alteration of any data inevitably causes unacceptable civilian harm (as it is the latter the principle of distinction is\textsuperscript{76} Heather A Harrison Dinniss, ‘The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives’ (2015) 48 Israel Law Review 39, 41.
\textsuperscript{77} Kubo Mačák, ‘Unblurring the Lines: Military Cyber Operations and International Law’ (2021) 6 Journal of Cyber Policy 411, 421–422. Denmark, Chile and Israel, on the other hand, insist on tangibility.
\textsuperscript{79} UK National Cybersecurity Centre (n 38). Note that if a civilian chooses to participate in sending such requests, this could have significant consequences regarding the question of whether they are targetable as civilians directly participating in hostilities. For a detailed discussion of this issue, see David Turns, ‘Cyber Warfare and the Notion of Direct Participation in Hostilities’ (2012) 17 Journal of Conflict and Security Law 279.
\textsuperscript{80} UK National Cybersecurity Centre (n 38).
meant to prevent). Especially when applying the principle of proportionality, a blanket interpretation of data as an object might be problematic since considering every deleted byte of civilian data as damage to a civilian object might quickly make an operation disproportionate even when the actual civilian harm is minimal, which will be explored in more detail below. Therefore, as with the re-interpretation of violence, there is a need to establish guiding criteria on how the deletion or alteration of data translates into civilian harm. Yet, the existing norms of LOAC as well as the academic literature on this issue seem to provide relatively little guidance on this issue.

More generally, all three avenues have one issue in common: they are helpful in the sense that they offer text- and purpose-based reasons for why even operations without violent effects must not be directed at civilians. However, they fall short in providing clear and sensible criteria to identify situations in which the non-violent effects of cyberoperations would translate into unacceptable civilian harm, thus requiring distinction. Before the emergence of cyber-based methods of warfare, ‘violence’ (understood as the creation of physical effects) might have been a reasonably accurate proxy for identifying such situations since (in absence of territorial control) physically destroying material civilian objects or injuring civilians was the only way to cause both direct material and significant immaterial harm to the civilian population. To find a similarly accurate proxy for cyberspace is necessary since cyber-systems and data do not merit humanitarian protection because of their inherent value, but rather due to their relevance to the well-being of the civilian population. However, as illustrated above, this relevance differs substantially between systems and data types, which makes general proxies like a loss of functionality or the deletion of any data seem inadequate. Consequently, a more dynamic framework might be required.

---

81 For instance, as discussed above, the value of a streaming service and the associated data clearly differs from that of an essential government service.
II. ‘UPDATE FAILED’? ENSURING THE APPLICABILITY OF THE
PRINCIPLE OF DISTINCTION IS INSUFFICIENT TO
EFFECTIVELY PROTECT CIVILIANS FROM HARM CAUSED BY
CYBEROPERATIONS WITHOUT PHYSICAL EFFECTS

Although it was shown that opinions as to which re-adjustments of the
existing law would be most desirable and acceptable differ widely, most
commentators seem to agree on one underlying assumption: the law of targeting
should be applicable because it would provide meaningful protection from
immaterial harms caused by military cyberoperations during armed conflict.
However, the rules of the law of targeting – most importantly the prohibition
on attacking civilians\(^\text{82}\) and civilian objects, the prohibition on disproportionate
attacks and the obligation to take all feasible precautions – were drafted with
conventional land warfare in mind.\(^\text{83}\) The following section will hence explore if
the law of targeting can still provide adequate protection if applied to operations
which do not produce reasonably foreseeable physical effects. This will allow an
assessment of whether the gap in legal protection alleged by many
commentators could, indeed, be remedied by interpreting extant LOAC in a way
that would ensure the applicability of the principle of distinction.

2.1.1 Distinguishing between military objectives and civilians objects in an interconnected
space

The UK has stated that ‘targeting can be challenging in
cyberoperations due to the potential dual use nature of some targets, such as
infrastructure’.\(^\text{84}\) While the identification of what qualifies as a lawfully targetable
military objective under Article 52(2) AP1 has always been difficult, the
interconnected nature of cyberspace might exacerbate these difficulties and lead

\(^{82}\) As operations without physical effects will, by definition, not injure or kill individuals,
the distinction between combatants and civilians will not be considered in the following.
Only if an individual’s data or online activities were conceived as their virtual self, would
a distinction between ‘virtual civilians’ and ‘virtual combatants’ become relevant to the
debate on cyber-contained operations. However, such an interpretation of cyber-activity
and -systems has not taken up a prominent place in the pertinent academic debates.
\(^{83}\) See Article 49(2) AP1.
\(^{84}\) Bannelier (n 2) 450.
to a situation ‘where nothing civilian remains’.\textsuperscript{85} Imagine a military base sending information to another base. Once the relevant communication packages leave the local network of the sending base, the bits that are being sent will most likely travel through cables and servers which are also used for civilian cyber-systems.\textsuperscript{86} This thereby makes it very difficult to separate civilian and military segments of cyberspace.\textsuperscript{87} To the extent that cyberspace is centralised with one ‘upstream’ server shifting information back and forth from both military and civilian ‘downstream’ devices, targeting a central server will offer a military advantage as it will impede communications between the connected military devices. Therefore, the server will qualify as a military objective by use. The acting party does not need to know exactly which routes the information will travel through; it is sufficient that it was reasonably likely that the targeted channel or server was used.\textsuperscript{88} Some commentators hence argue that ‘in theory, a country’s entire cyber infrastructure could be qualified as a military objective once engaged in armed conflict’.\textsuperscript{89}

In some way, this problem can be seen as a corollary of the fact that cyber-contained operations, by definition, only affect the code and content layers of cyberspace.\textsuperscript{90} Prominent models of cyberspace, like for instance the Open Systems Interconnection Model (OSI-model), highlight that cyberspace is not a monolithic structure, but a complex aggregate of different layers.\textsuperscript{91} It should be noted that the seven layers of the OSI-model were designed for a different purpose than to legally classify attacks and are sometimes difficult to distinguish in practice. Nevertheless, they are useful with respect to the questions addressed in this article as they allow a disaggregation of cyberspace

\footnotesize
\textsuperscript{85} Droege (n 37) 565; Elaine Korzak and James Gow, ‘Computer Network Attacks under the Ius Ad Bellum and the Ius in Bello - Distinction, Proportionality, Ambiguity and Attribution’, Routledge Handbook of War, Law and Technology (Taylor & Francis 2019) 77–78.
\textsuperscript{88} NATO Cooperative Cyber Defence Centre of Excellence (n 2) 446.
\textsuperscript{89} Korzak and Gow (n 85) 77–78.
\textsuperscript{90} On the three layers of cyberspace, see Andrew Murray, The Regulation of Cyberspace: Control in the Online Environment (Routledge-Cavendish 2006) 54.
into a physical layer and other non-physical layers. While physical cyber-infrastructure is as geographically locatable as any other material target, the code and data making up the non-physical layers of cyberspace are harder to conceptualise as targetable entities in a space since they are nothing more than constantly moving electrons.\textsuperscript{92} Although it will sometimes be technically feasible to single out specific sub-systems as targets,\textsuperscript{93} the general idea of ensuring protection through distinction is based on the assumption of identifiable and separable targets. For this assumption to hold, a significant re-conceptualisation of either the non-physical components of cyberspace or the principle of distinction seems necessary.

Consequently, one might argue that even if the principle of distinction was applicable to operations without physical effects, the interconnected and dual-use nature of cyberspace would make the prohibition on directly attacking civilian objects less relevant. As many virtual components of cyberspace which are also integral for civilian use are likely to qualify as military objectives,\textsuperscript{94} the aspired separation between a predominately military sphere and a predominately civilian sphere becomes increasingly tenuous. Under current LOAC, cyberspace can be conceived of as part of the former sphere based on its pivotal role for the conduct of (both virtual and kinetic) military operations, despite still being overwhelmingly civilian. This ‘legal militarisation’ of cyberspace runs counter to the overall idea of distinction, namely, to limit attacks to spaces used predominantly by the military.

The concrete legal consequence of this would be that targeting vast parts of cyberspace would be compatible with the prohibition on targeting civilian objects. Civilians would hence not be protected from such operations as such, but only from excessive effects thereof and by the obligation of commanders to take all feasible precautions to prevent such a disproportionate

\textsuperscript{93} In fact, if possible, there is an obligation to do so, according to the TM experts; NATO Cooperative Cyber Defence Centre of Excellence (n 2) 470.
\textsuperscript{94} Terry D Gill, Jelle van Haaster and Mark Roorda, ‘Some Legal and Operational Considerations Regarding Remote Warfare: Drones and Cyber Warfare Revisited’ in Jens Ohlin, Research Handbook on Remote Warfare (Edward Elgar Publishing 2017) 326.
impact. Accordingly, the heavy lifting of protection would have to be done by the principles of proportionality and precaution.\(^{95}\)

2.1.2 Applying the principles of proportionality and precaution in a complex space

With this conclusion in mind, can the principles of proportionality and precaution be applied to cyberoperations without physical effects in a way that meaningfully limits their impact on civilians? Both principles are crucial to ensure the protection of civilians since they oblige belligerent parties to try to minimise incidental civilian damage while planning and executing operations, and oblige them to refrain from operations that would cause excessive incidental physical harm to civilians. According to the principle of proportionality, as stipulated in Article 51(5)(b) AP1, attacks ‘which 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’ are unlawful. The principle of precaution further obliges commanders to ascertain the military nature of their target,\(^{96}\) give warnings to civilians if possible,\(^{97}\) and to ‘take all feasible precautions in the choice of means and methods of attack with a view to avoiding, and in any event to minimising, incidental loss of civilian life, injury to civilians and damage to civilian objects’.\(^{98}\) Furthermore, ‘[w]hen a choice is possible between several military objectives for obtaining a similar military advantage’, the target minimising incidental harm shall be chosen.\(^{99}\) Even before planning a specific attack, Article 58 AP1 further sets out general precautionary measures aimed at minimising the incidental impact of military operations on civilians, like the removal of civilians from areas close to military objectives\(^{100}\) or avoiding the placement of military objectives in the vicinity of densely populated areas.\(^{101}\) One commentator claims that, in principle, these rules apply in the same way to cyberoperations as they do to kinetic operations.\(^{102}\) This is correct in the sense that the general problems of the principles of proportionality and precaution are

\(^{95}\) Geiß and Lahmann (n 86) 398.
\(^{96}\) Article 57(2)(a)(i) AP1.
\(^{97}\) Article 57(2)(c) AP1.
\(^{98}\) Article 57(2)(a)(ii) AP1.
\(^{99}\) Article 57(3) AP1.
\(^{100}\) Article 58(a) AP1.
\(^{101}\) Article 58(b) AP1.
\(^{102}\) Gill (n 11) 468.
equally pertinent when applied to cyberoperations. However, the following subsection will illustrate how there are three factors aggravating existing challenges\(^\text{103}\) and adding new ones.

First, cyberspace is highly complex. It might not always be straightforward to understand how devices are connected and how they communicate.\(^\text{104}\) In many cases, the full impact of an operation will only show after a long time,\(^\text{105}\) which makes both the application of Article 57(2)(a) and Article 57(2)(b) AP\(^\text{1}\) exceptionally difficult. Additionally, the software used by the devices to which a targeted cyberoperation was initially tailored is constantly changing, for instance, due to software updates or minor corrections of coding errors. A malware that might be controllable and spread only within a specific subsystem based on a digital signature (integrated in the software of the devices it is meant to disable) could spin out of control if this signature is removed by a software update, and the malware hence no longer ‘sees’ the difference between devices it is meant to disable and those that should be left unharmed.\(^\text{106}\)

Second, the direct effects of a cyberoperation on civilian devices and services might be highly heterogeneous because of their differing susceptibility to a specific operation. Coming back to the aforementioned example, malware might only affect users who have already updated their software to the latest version. Consequently, unlike a bomb which severely damages every house it is dropped on, the direct effects of cyberoperations can be highly heterogeneous

\(^{103}\) For instance, from a practical perspective, one commentator laments an information asymmetry between commanders and judicial or other bodies scrutinizing their decisions with a view to the principle of proportionality, especially the expected civilian damage and the anticipated military advantage; David Luban, ‘Military Necessity and the Cultures of Military Law’ (2013) 26 Leiden Journal of International Law 315, 326–327. From a legal perspective, it is unclear how exactly a military advantage and incidental civilian harm can be compared, and at which exact point the latter becomes excessive; Pilloud and others (n 52) 625.

\(^{104}\) Roscini (n 62) 95.

\(^{105}\) Bannelier (n 2) 439.

and depend on the targeted system.\textsuperscript{107} This will make it hard to precisely assess the effects of an operation \textit{ex ante}.

Third, assuming for the sake of argument that ‘damage’ is not limited to physical effects or that ‘objects’ includes intangible data, an additional challenge emerges. If non-physical harm is considered, one might wonder how to quantify the damage caused by an operation. Some commentators argue that any loss of functionality should be considered as damage under Article 51(5)(b) AP\textsuperscript{1} because anything else would make the prediction of damage practically impossible.\textsuperscript{108} Yet, this elevates the legal protection of cyber-systems to an end in itself, which it arguably is not. The real harm is not the dysfunctions or loss of data as such, but the impossibility of using cyberspace or data to enjoy certain freedoms. Consequently, this protection is a means to ensure that civilians can enjoy certain immaterial goods and undertake certain activities.

Given that the actual harm caused to civilians by cyberoperations without physical effects is used as a key argument in favour of moving away from a strict focus on physical damage,\textsuperscript{109} it would seem inconsistent to then ignore this actual harm and instead just assume that each loss of functionality or deletion of data will affect civilians in the same way. Yet, if one moves away from this assumption, the assessment of damage would require a ‘translation’ of the inaccessibility of cyber-systems or data into actual harm. This seems problematic as the final harmful effects on civilians’ lives of an operation are likely to differ greatly depending on individual habits, use patterns and the overall dependence on cyber-based services. Imagine an operation disabling a messaging service. If a civilian uses this service to communicate with their family or receive information on the availability of humanitarian aid, they will be greatly affected. Their neighbour, using a different service, might not even become aware of the operation. This example shows that the above-mentioned

\begin{thebibliography}{9}
\bibitem{108} Geiß and Lahmann (n 86) 397.
\bibitem{109} Lubell (n 36) 275.
\end{thebibliography}
‘translation’ might depend on highly individualised features and will hence infinitely complicate an *ex ante* assessment of expected damages.\(^{110}\)

This analysis needs to be caveated with respect to one aspect of the principle of precaution: the separation of civilian and military infrastructure (Article 58(b) AP1). Although a complete separation is neither legally required, nor realistic,\(^ {111}\) the TM lists various preventative measures that states might take, e.g., creating back-ups for essential civilian datasets or promoting antivirus measures to protect civilian systems.\(^ {112}\) Such measures seem more feasible than the active precautions addressed above since they do not require an assessment of the precise effects of a specific operation. At the same time, they could prevent the emergence of many harmful effects in the first place by making them technologically impossible or more unlikely, which makes such measures a crucial avenue for protection.

In sum, one might caution that the difficulties of applying the principles of distinction, proportionality and precaution to cyberoperations without physical effects might turn the respective norms, assuming they are applicable, into ‘licensing tools’ (i.e., norms allowing states to legitimise their actions with reference to its lawfulness without actually limiting their discretion in deciding how to conduct hostilities).\(^ {113}\) As explicated above, most of cyberspace could reasonably be construed as a military objective, and anticipating the incidental harm caused by an operation here is especially difficult. Consequently, even for operations which will have a substantial impact on the civilian use of cyberspace, states might reasonably argue that they were targeting a military objective and assess potential collateral effects to the best of their abilities. As one commentator put it, ‘this kind of ‘normative

\(^{110}\) Note that this is not to say that this problem is equally relevant for all kinds of operations. For instance, an operation affecting transportation services needed to flee from kinetic hostilities will have a relatively homogenous effect on everyone in a certain region. However, there will be operations, like the previously mentioned example, that create highly heterogenous effects, making an estimation of the expected incidental harm highly speculative.

\(^{111}\) Droege (n 37) 567.

\(^{112}\) NATO Cooperative Cyber Defence Centre of Excellence (n 2) 488.

indeterminacy” gives belligerents a large margin of appreciation,114 potentially allowing them to hide from political or moral judgment behind the cloak of plausible legality. Hence, one might wonder how much would actually be gained by making the principles of distinction, proportionality, and precaution applicable – and what might be lost.

III. ‘PLUGIN AVAILABLE’? CIVILIANS MIGHT BENEFIT FROM AN INCREASED FOCUS ON INTERNATIONAL HUMAN RIGHTS LAW

Another assumption that seems to underlie large parts of the above debates is that LOAC is the only body of international law that could provide protection. Arguing that the inapplicability of the principle of distinction causes a gap in protection implies that no other body of law is filling this gap left by LOAC.115 This assumption will be challenged with reference to IHRL.

3.1 Could human rights be the more adequate regime to regulate cyberoperations without physical effects?

Due to its origins as a ‘peacetime law’,116 IHRL is far less focused on violent hostilities than LOAC, and especially the law of targeting. Consequently, the protection it provides is inspired by a fundamentally different logic.117 Instead of prohibiting certain actions, it formulates rights that need to be respected, protected, and fulfilled by states. Hence, IHRL directly protects immaterial values, i.e., rights. This foundation makes IHRL highly relevant to cyberoperations without physical effects since they are liable to precisely impact such immaterial values. Three examples can help to illustrate this point.

First, consider an operation against the head of government of the enemy belligerent party whose private phone calls are intercepted and then

---

114 Bannelier (n 2) 437.
115 This assumption is further reflected by the focus on LOAC in the academic literature. For instance, the Tallinn Manual discusses LOAC on 189 pages and human rights on 30.
published online to humiliate her. Such an operation is likely to engage the right to private life which has been interpreted by human rights bodies to also encompass the protection of personal data and the privacy of communications. In absence of a derogation or a legitimate exception based in law, the publishing of personal data, images or communications would thus be liable to constitute a violation of the right to private life.

Second, a party might decide to block access to all major news portals. As the internet is increasingly recognised as an important means of exercising the right to freedom of expression, such an operation could constitute a breach of this right. To illustrate: in a case without a nexus to armed conflict, the European Court of Human Rights assessed the legality of a national court order mandating a block on access to a Google service which allowed users to upload content on their websites. The Court argued that this was the only way to prevent access to certain websites which contained content allegedly insulting the memory of Atatürk. The Court considered that the blocked service was ‘designed to facilitate the creation and sharing of websites within a group and thus constitutes a means of exercising freedom of expression’. It ruled that the court order constituted a violation of Article 10 of the European Convention of Human Rights (ECHR).

Third, imagine an operation to delete the online banking information of millions of civilians. As a result, they are unable to access their funds for several weeks and might even permanently lose certain assets. This will certainly have a negative impact on their ability to enjoy their possessions and potentially

119 S and Marper v the United Kingdom [2008] App no 30562/04, 30566/04 (ECtHR, 4 December 2008) [41].
120 This resembles certain operations during the Estonia 2007 incident (see above).
121 See, e.g., Delfi as v Estonia [2015] App no 64569/09 (ECtHR, 16 June 2015) [110].
122 Ahmet Yildirim v Turkey [2012] App no 3111/10 (ECtHR, 18 December 2012) [7–11].
123 ibid 51.
124 ibid 49.
125 ibid 72.
even amount to expropriation. Consequently, the right to property might be engaged.

The goal of these examples is not to argue that all these operations would definitely amount to violations of IHRL. They are merely meant to show that IHRL covers a wide range of operations without physical effects, which would not be covered under LOAC if a traditional understanding of violence and objects is maintained since IHRL directly protects the enjoyment of certain rights of freedoms that might be affected by military cyberoperations during armed conflict. More broadly, IHRL might have some generally advantageous features.

Section three of this paper showed that rigid prohibitions might fall short of accounting for the versatile relationship between the direct effect of an operation and its overall consequences for civilian lives. One might argue that this rather rigid and conduct-based nature of the law of armed conflict is the only way to cut through ‘the fog of war’, i.e., the opaqueness emanating from the extreme pressures and dynamic of armed conflict. However, this argument does not apply in the same way to cyberoperations as it does to traditional operations on a physical battlefield. Cyberoperations require meticulous planning and can usually be conducted far away from the physical battlefield. Hence, it would seem conceivable for commanders to take more nuanced rules into account. IHRL’s rights-based nature allows for a dynamic application of the law as it does not outlaw specific behaviours which are generally likely to cause a certain level of harm, but rather directly protects certain rights, which are then assessed in light of specific state action. As each cyberoperation produces very specific effects, this outcome-based logic might be a better fit than LOAC’s general prohibitions.

Moreover, IHRL’s focus on the individual as a rights-holder and the access to legal remedies (most importantly, court proceedings and potentially reparations) might be an appropriate response to the above-mentioned differential effects of cyberoperations. Given the great difficulties in assessing the precise effects of an operation, even in the aftermath of an incident, it might be

126 Sporrong and Lönnroth v Sweden [1982] App no 7151/75, 7152/75 (ECtHR, 23 September 1982) [61].
127 Luban (n 103) 627–628.
sensible to make the individual the relevant unit of analysis and allow for individuals to come forward with complaints regarding how a specific operation has affected them.

Additionally, states would be required to explain why certain operations were necessary to pursue a legitimate aim or were strictly required by the exigencies of a situation. It is important to emphasise that IHRL would still allow states to derogate from or limit their human rights obligations for security reasons. However, instead of relying on blanket justifications, states would have to show that their derogation or interference was strictly required or necessary to pursue a legitimate aim. As the burden of proof regarding the lawfulness of an interference or derogation is on the state party, the application of IHRL might help to ensure a transparent account of how the cyberoperation affected civilians and whether this was strictly necessary. Although states might be reluctant to share the details of why they took a specific measure with reference to the confidential nature of national security, they will have to at least make a generally reasonable case for how an operation was linked to a threat to their security and why the resulting harm to civilians was necessary. While human rights law in general is plagued by an information asymmetry between states and courts in this respect, the mere fact that a case or incident would be discussed in a public forum would make cyberoperations subject to a level of attention and scrutiny, including from civil society actors, which would otherwise be unlikely.

Of course, the details of which institution would deal with claims by individuals, and how exactly it would do so, depends on which IHRL treaty is relied on. While a detailed analysis of specific human rights regimes is beyond the scope of this article, all human rights treaties have some sort of complaint mechanism, albeit differing in their level of enforceability and degree of judicialisation, that could allow for state accountability. The fact that some could

---

128 Article 4(1) ICCPR; Article 15(1) ECHR.
do so more effectively than others\footnote{For instance, the ECtHR is certainly exceptional in terms of enforceability since the judgments of the ECtHR are binding upon parties to a specific case (Article 46(1) ECHR) and a failure to abide can entail sanctions (Article 46(5) ECHR).} does not take away from the general observations presented in this article.

In sum, IHRL’s focus on individual rights, accountability and transparency could help resolve many of the challenges outlined above with regards to LOAC.

3.2 Problems of applying human rights law

While it was argued that IHRL potentially covers many operations which are likely to escape the reach of LOAC as it stands, human rights’ actual protective value depends on one crucial question: is IHRL applicable? For state-conducted cyberoperations, there are two main potential reasons for inapplicability.\footnote{In an analysis not limited to state operations, the limited binding effect of IHRL on non-state actors would constitute another such reason. While the legal attribution of cyberoperations conducted by non-state actors to states is beyond the realm of this article, it would need to be explored in an analysis aiming at finding a final verdict on the usefulness of human rights law regarding cyberoperations with a nexus to armed conflict.}

3.2.1 The relationship between LOAC and IHRL

The relationship between LOAC and IHRL is a perennial issue. Ever since the International Court of Justice’s (ICJ) Advisory Opinion on the \textit{Legality of the Threat or Use of Nuclear Weapons}, there can be no doubt that, in principle, IHRL can apply even in times of armed conflict.\footnote{International Court of Justice, ‘Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion’ International Court of Justice Reports 1996 [25] <https://www.icj-cij.org/public/files/case-related/95/095-19960708-ADV-01-00-EN.pdf> accessed 16 February 2023.} In its \textit{Wall Advisory Opinion}, the Court further specified that LOAC does not displace IHRL in general. Instead, ‘some rights may be exclusively matters of international humanitarian law; others may be exclusively matters of human rights law; yet others may be matters of both these branches of international law’.\footnote{International Court of Justice, ‘Legal Consequences of the Construction of a Wall, Advisory Opinion’ International Court of Justice Reports 2004 [106]} Still, there remains
ambiguity in how IHRL and LOAC interact in practice. While several ways of conceptualising this interaction are imaginable, the following discussion will focus on two approaches that are most frequently discussed in the pertinent literature: the *lex specialis* approach and the *belt and suspender* approach. The supporters of the so-called *lex specialis* approach argue that LOAC generally supersedes IHRL as the more specific law in times of armed conflict, unless an issue is not dealt with in the pertinent LOAC treaties. The alternative *belt and suspender* approach sees LOAC and IHRL on a more equal footing and accords priority to the body of law providing a higher level of protection in a specific situation. While a full discussion of this issue is beyond the scope of this essay, the specific phenomenon of cyberoperations without physical effects creates an interesting constellation.

Assuming that the law of targeting only applies to acts with reasonably foreseeable physical effects and the law of occupation does not apply, one
might argue that there is a gap in LOAC that can be filled by IHRL. Potential conflicts between LOAC and IHRL have often been identified with a view to the right to life and detention.\textsuperscript{139} The class of operations considered in this work, \textit{by definition}, does not fall within these areas as they do not foreseeably impact the right to life, physical integrity or free movement.

On the other hand, should the interpretation of the law of targeting evolve to include cyberoperations without physical effects, the rules of LOAC might take precedence under a \textit{lex specialis} approach. If one agrees with the above analysis of the potential shortcomings of LOAC with respect to cyber-contained operations, this dynamic could be seen as another reason to carefully consider the desirability of making the law of targeting applicable to such operations.

However, even if the law of targeting, indeed, were to ‘pull its anchor’ of physical effects, IHRL might still supersede LOAC if it provides more protection under the alternative \textit{belt and suspender} approach.

This essay argues that this could very well be the case.\textsuperscript{140} Yet, this would require a rule-by-rule analysis of which rule provides more protection. Given that this depends greatly on the definition of ‘protection’ and the speculated effect of applying a specific norm, there might not always be a clear outcome of such an assessment. Accordingly, this would be a less clear-cut approach than applying IHRL as the more specific law to a situation on which LOAC is silent, which would be possible if the law of targeting remains limited to cyberoperations with physical effects. In the latter case, there would be no issue of conflicting or overlapping norms between LOAC and IHRL and hence no merit in arguments purporting that LOAC supersedes pertinent IHRL guarantees.

\textsuperscript{139} On the right to life, see Droege (n 117), 344-347. On detention, see Lubell (n 135) 657.

\textsuperscript{140} A detailed analysis would be required to assess if a similar conclusion can be drawn regarding the law of occupation. For a detailed and critical discussion of applying human rights to cyber-based operations in situations of occupation, see Omar Yousef Shehabi, ‘Emerging Technologies, Digital Privacy, and Data Protection in Military Occupation’ in Russell Buchan and Asaf Lubin (eds), \textit{The Rights to Privacy and Data Protection in Times of Armed Conflict} (NATO CCDCOE Publications 2022).
It should be noted that aside from approaches emphasising the need to determine when LOAC supersedes IHRL and vice versa, the relationship between IHRL and LOAC can also be perceived as one of complementarity.\textsuperscript{141} This would entail a focus on finding conciliatory interpretations allowing the two bodies of law to ‘influence and reinforce each other mutually’.\textsuperscript{142} In fact, it has been argued that most courts have interpreted the *lex specialis* approach to resolve norm conflicts in a way that closely resembles the interpretative principle of systematic integration.\textsuperscript{143} This principle is based on Article 31(3)(c) VCLT, which allows for the consideration of any ‘relevant rule of international law applicable in the relations between the parties’ and is based on the idea that international law should form a coherent set of rules.\textsuperscript{144} In the context of this article, the idea of systematic integration is pertinent in resolving some of the interpretative questions and challenges outlined in the two previous sections. To mention a specific example, the term ‘damage’ under LOAC could be interpreted in a way that focuses on the effect on the enjoyment of human rights of a specific operation. A similar proposal could be formulated on the question of which types of data should be protected as civilian objects, namely those which are also protected by human rights guarantees (e.g., the right to private life). In this sense, the challenge of defining and quantifying harm when exclusively focusing on existing norms of LOAC could be mitigated by borrowing from IHRL treaty and case law. However, this approach is premised on the assumption that LOAC and IHRL are generally placed on an equal footing, even during armed conflict. Although certainly relevant in the context of this article, the principle of systematic integration remains a principle of interpretation aimed at reducing situations in which LOAC and IHRL are in conflict with each other, not one of deciding which rule takes precedence for the cases where they still do.

\textsuperscript{141} Droge (n 117) 340-344.
\textsuperscript{142} Droge (n 117) 337.
\textsuperscript{144} Campbell McLachlan, ‘The Principle of Systematic Integration and Article 31(3)(c) of the Vienna Convention’ (2005) 54 International and Comparative Law Quarterly 279, 626; Droge (n 117) 227.
3.2.2 ‘Physically’ strikes back: extraterritorial application of human rights treaties

An equally critical question regarding the applicability of IHRL might be related to its territorial scope. In non-international armed conflict (NIAC), the affected individuals will most likely remain within the territorial jurisdiction of the belligerent state, where the latter is clearly bound by its human rights obligations.\(^\text{145}\) On the other hand, in international armed conflict, most operations will most likely affect individuals in the enemy state’s territory, who are not necessarily within the acting state’s jurisdiction.\(^\text{146}\) Consequently, questions pertaining to the extraterritorial applicability of human rights obligations are likely to play a decisive role in determining the protective reach of IHRL.

While positive obligations to protect will bind the belligerent party on whose territory fighting takes place,\(^\text{147}\) an attacking belligerent party acting on foreign territory could potentially not be bound by its negative obligations to respect human rights. Since IHRL protections are far more developed in treaty law, the clauses on territorial application in the respective treaties are crucial in this respect.\(^\text{148}\) Whereas the International Covenant on Social, Economic and Cultural Rights does not have an explicit territorial limitation, the International Covenant on Civil and Political Rights (ICCPR) and the European Convention on Human Rights (ECHR) apply only to persons within the jurisdiction of the contracting party.\(^\text{149}\)

Although some states claim that this strictly limits their human rights obligations to their territory,\(^\text{150}\) the majority of scholars and the most important

\(^{145}\) The ECtHR established the assumption that persons in the territory of a Contracting Party are under its jurisdiction, which can only be rebutted in exceptional circumstances. *Ilaşcu and Others v Moldova and Russia* [2004] App no 48787/99 (ECtHR, 8 July 2004) [312].

\(^{146}\) A more complicated scenario would be an ‘internationalised NIAC’ in which foreign forces fight on behalf of the government or insurgent forces. In this case, there would be a need to analyse if the intervening foreign forces are bound by their state’s human rights obligations.

\(^{147}\) These obligations have been discussed in detail elsewhere; see, *inter alia*, Berkes (n 92) 227–230.

\(^{148}\) NATO Cooperative Cyber Defence Centre of Excellence (n 2) 186.

\(^{149}\) Article 1 ECHR, Article 2(1) ICCPR.

\(^{150}\) Gaggioli (n 116) 154.
human rights bodies concur that extraterritorial obligations exist. However, they remain an exception and are limited to very specific situations. For instance, the case law of the European Court of Human Rights primarily suggests five situations of extraterritorial applicability: all cases of lawful and unlawful occupation, specific acts of (physical) violence involving an element of proximity, actions taken by diplomatic and consular agents abroad, exercises of extra-territorial public powers at the invitation or with the acquiescence of a foreign state and situations in which a state has effective control over a person or territory of a foreign state. The final situation can be understood as physical control over territory or a person. The Court had stated earlier that the ECHR does not apply to airborne operations with lethal effects outside the European legal space. In fact, it explicitly rejected a ‘cause-and-effect’ notion of territorial applicability similar to that of the Geneva Conventions.

If applying an ‘effective control’ standard or similar theories, it is unlikely that a cyberoperation would trigger extraterritorial human rights obligations unless it affects persons detained by the belligerent party or are situated in occupied territories. However, since cyberoperations do not require physical control over territory or persons to produce significant effects on the enjoyment of rights by people in this territory, human rights treaties might remain inapplicable in situations where cyberoperations produce significantly harmful effects in territories which are not under effective control of the acting belligerent party.

---

151 ibid 155.
152 Loizidou v Turkey [1996] App no 15318/89 (ECtHR, 18 December 1996) [52].
153 Georgia v Russia (ii) [2021] App no 38263/08 (ECtHR, 21 January 2021) [130–131]; Carter v Russia [2021] App no 20914/07 (ECtHR, 21 September 2021) [129].
156 On the spatial model, see Milanovic (n 129) 127–173. On the personal model, see ibid 173–209.
The majority of the TM experts equally considered physical control over either territory or individuals as a necessary premise for human rights to apply extraterritorially. To support this view, they cited the reluctance of many states to apply IHRL to their intelligence operations targeting foreigners abroad.\(^{157}\) However, it should be noted that the US submitted their intelligence programme to human rights obligations at least as a matter of policy.\(^ {158}\) A similar move had also been proposed by several states in a draft UN General Assembly resolution.\(^ {159}\) Although these developments fall short of establishing extraterritorial obligations for states under the law as it stands, they might still be interpreted as evidence for a general willingness to reconsider the territorial scope of international human rights law with respect to cyber-based behaviour. Moreover, it might be noteworthy that states increasingly tend to extend their jurisdiction to foreigners when regulating online platforms.\(^ {160}\) While there is a great difference between general jurisdiction and jurisdiction as the delimiter of the territorial scope of human rights obligations, this development might nevertheless signify a general trend towards a less territorial understanding of jurisdiction in the context of cyber-activities.

Such an evolution would be in line with the *sui generis* nature of cyberspace. While the infrastructure making up the physical layer of cyberspace can be assumed to be under the exclusive control of one state,\(^ {161}\) the code and content layer of cyberspace are hard to fit into the Westphalian model of
territorially grounded sovereignty. While servers and cables are located in one place, computer commands and online content are nothing more than electrical signals travelling within milliseconds from one device or server to another. Therefore, it will be very difficult, if not impossible, to use their physical location as a way of deciding which laws apply. Although it would be premature to derive any consequences for the applicability of human rights lex lata from this observation, it might nevertheless serve as a strong argument in favour of reconsidering existing concepts on the extraterritorial application of IHRL. In fact, a minority of the TM experts argued that ‘so long as the exercise or enjoyment of a human right in question by the individual concerned is within the power or effective control of a State’, human rights law should apply. Furthermore, it should be noted that the ECtHR recently held that ‘[t]he extent of the State’s obligations under Article 1 of the Convention is to secure to [an] individual the Convention rights and freedoms that are relevant to his or her situation’. While this holding did not relate to cyber-based conduct, it could nevertheless be seen as a sign that the ECtHR is willing to move towards a more flexible, effects-based approach to extraterritorial applicability.

This is not to say that such an approach would be entirely unproblematic. The ECtHR in Banković expressed the fear that a ‘cause-and-effect’ notion of extraterritorial applicability would fragment the applicability regime of the Convention into several pieces that are specifically tailored to the particular circumstances of an extraterritorial act, hence negatively impacting the integrity of the Convention. Furthermore, there might be a need to distinguish between positive and negative obligations, with

---

164 NATO Cooperative Cyber Defence Centre of Excellence (n 2) 185.
165 Ukraine and the Netherlands v Russia (dec) [2022] App no 8019/16, 43800/14, 28525/20 (ECtHR, 30 November 2022) [571].
166 Banković and Others v Belgium (n 155) para 75. Note, however, that this conclusion has recently been explicitly overruled by the Court in its admissibility decision on applications arising from the conflict between Russia and Ukraine; Ukraine and the Netherlands v. Russia (dec.) (n 165) para 571.
only the latter applying extraterritorially based on the effect of a state act.\textsuperscript{167} If any act of a state having some effect on an individual in another state triggered obligations to protect and to fulfil the human rights of said individual, this could lead to conflicts with state sovereignty and overwhelm individual states.\textsuperscript{168} Additionally, if any type of extraterritorial effect were to trigger the applicability of human rights treaties, the respective courts and mechanisms might quickly be overwhelmed by a flood of claims.\textsuperscript{169}

Despite these challenges, the above considerations regarding the desirability of applying human rights law to military cyberoperations lead this author to conclude that debates on military cyberoperations should not only focus on updating LOAC to present-day warfare, but also consider the need to adapt human rights law to the unique nature of cyberspace. As IHRL protects immaterial goods, it is apt to close gaps in legal protection left by LOAC's focus on physicality. However, it can only do so if it is applicable. This is currently not the case when a state uses cyberspace to cause harm in the territory of an enemy belligerent state. This author believes that there is a need to extend the applicability of IHRL to such conduct so as to ensure the full enjoyment of human rights.

\textbf{IV. THE WAY AHEAD: A PLEA TO BROADEN THE DEBATE ON MILITARY CYBEROPERATIONS WITHOUT PHYSICAL EFFECTS}

Sections two and three explicated why the most prevalent rules of the law of targeting are not easily transferable to cyber-contained operations. Section four argued that IHRL's rights-based approach might be more apt to the specific challenges of such operations but conceded that its utility in IAC is strongly circumscribed by its limited territorial applicability.

Hence, this author concurs with many scholars that a gap in protection exists. However, the above discussions suggest that it is not a lack of physical effects alone which causes a gap in protection. Instead, combining the results of

\textsuperscript{168} Milanovic (n 129) 219.
\textsuperscript{169} ibid 221.
the preceding sections, the root of the problem can be traced back to an underlying assumption shared by both LOAC and IHRL: immaterial values/rights can only be *directly and significantly* restricted if a party has physical control over persons or territory.

4.1 The real problem: The relation between virtual and physical space

It would be an oversimplification to suggest that the LOAC as a whole is ‘physically anchored’. In fact, non-material values are protected by several provisions: Article 75(2)(b) AP1 protects against outrages upon personal dignity, Article 25 Geneva Convention IV (GCIV) protects communications with family members, Article 27 GCIV guarantees protected individuals ‘respect for their persons, their honour, their family rights, their religious convictions and practices, and their manners and customs’. All these provisions have two commonalities: they directly protect human dignity and they all only apply once a person is ‘in the hands’ or ‘in the power’ of a belligerent party. This shows that LOAC does in fact provide direct protection to non-material goods, but it limits such protection to situations where the belligerent party has physical control over a person or the territory this person finds themselves in.

Against this background, the discussions on Article 54 AP1 shed new light on the function of the term ‘attack’. Initially, the ICRC had proposed two quasi-identical provisions on the protection of objects indispensable to the survival of the civilian population. One was placed in the section on the general protection of the civilian population against the effects of hostilities, the other one was placed in the section on the treatment of persons in the power of a party to the conflict. The former (draft Article 48) stated that it was ‘forbidden to *attack* or destroy’ certain indispensable objects, whereas the latter (draft

---


171 See Article 4(1) GCIV and Article 75(1) AP1.

172 Pilloud and others (n 52) 47; ibid 866.

173 Given the persistent unclarity and potentially absurd conclusions regarding Article 49(1) AP1 outlined in section 2, a recourse to the preparatory work under Article 32 VCLT seems warranted.

174 One might be confused by the mentioning of both ‘to attack’ and ‘to destroy’. However, this does not imply that to attack and to destroy were considered mutually exclusive concepts. Diplomatic Conference on the Reaffirmation and Development of
Article 66) made it unlawful to ‘destroy, render useless, or remove objects indispensable to the survival of the civilian population’, which resembles the functionality approach proposed by some scholars with respect to cyber-contained operations. The difference between the two draft provisions was explained by an ICRC representative in the following terms: ‘The words “to attack” were not included in draft Article 66 because one did not attack what was in one’s possession’.\(^{175}\) This shows that the drafters assumed that attacks are only mounted by the party which is not in control of the objects or persons it is attacking. Any protection against attacks would hence only include those goods and values which were directly targetable while a party is not in control of the objects and persons targeted. In 1977, when the Additional Protocols to the Geneva Conventions were adopted, the private and family life of an individual (including the possibility to communicate), their personal dignity and other non-material goods, in absence of physical control over a person or territory, were only indirectly targetable via the physical destruction of certain objects required to give effect to them. Outlawing acts of violence targeting or excessively affecting civilian objects hence automatically also covered such non-material goods and liberties. Yet, this protection is always translated into the only way in which a belligerent party could impact civilian life in absence of territorial control: violence. As immaterial aspects of civilian life move online and become directly targetable through cyber-means, a mere extension of the scope of the law of targeting might not be sufficient since the actual harm caused by cyberoperations without physical effects simply cannot be translated into the language of violence and objects. Even if the existing rules were applicable, their protective value might be greatly diminished by the challenges faced when trying to apply the rules that were meant to protect material objects to the protection of immaterial objects and values more broadly. In this way, their protective value might be ‘lost in translation’.

In short, the author avers that there is a need to interpret the focus on physicality in the law of targeting, not only as a result of the means and methods of warfare known at the time when the Geneva Conventions and their Protocols were drafted. Instead, it should also be seen as a consequence of the drafters’ implicit assumptions about how civilian life can possibly be affected by a

\(^{175}\) ibid, para 36.
belligerent party in the absence of physical control. Consequently, not only the notion of ‘violence’, but also the concept of having ‘control over a person’ need to be taken into account when trying to ensure that civilians are as well protected from offline as from online harms.

This article has explored whether IHRL might close gaps in the legal protection provided by LOAC arising from the previously discussed features. It is concluded that its capacity to do so is limited by a similar assumption. IHRL is based on the idea that individuals have certain rights which can potentially be limited by the state since the latter has the monopoly of force with regards to the individuals within its territory. As a result of this power, a state has positive and negative obligations to ensure the enjoyment of these rights. While IHRL is conceptually more apt to regulate the harm caused by cyberoperations without physical effects since it protects immaterial values, a corollary of IHRL’s focus on a state’s ability to limit or facilitate the enjoyment of human rights is that its applicability is limited to situations where a state actually is ‘in power’.176 The latter notion has been interpreted by many human rights bodies as physical control over a person or territory. This author hence concludes that protection could be provided by IHRL, if it did not rely on the same fundamental notion as LOAC does: to be able to affect a person’s rights and freedoms, a state must have physical control over that person.

Cyberspace, however, allows parties to have remote control over the virtual space in which important aspects of civilian lives (communications, political participation, access to property and essential services, etc.) manifest without any physical control. In the view of the author, this is the actual novel feature of cyberspace causing a gap in legal protection from cyberoperations without physical effects. To legally and practically close the existing gap in protection, there would hence be a need to combine IHRL’s direct and comprehensive protection of immaterial goods and the law of targeting’s recognition that states also have to respect the civilian population of areas over which they have no effective control during armed conflict.

176 Droege (n 117) 335.
4.2 Possibility of an integrated approach?

Consequently, it seems reasonable to look for ways to ‘fold IHRL into LOAC’. Two potential avenues for integrating IHRL into LOAC in certain respects will be briefly discussed here: legal weapon reviews and the Martens Clause.

4.2.1 Legal reviews of cyberweapons

‘In the study, development, acquisition or adoption of a new weapon, means or method of warfare’, parties to AP1 are ‘under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party’. The wording of Article 36 AP1 suggests that this review is to be undertaken by states with a view to their weapons, means or methods of warfare’s compatibility with all their obligations under international law. The review is consequently not limited to LOAC but could also include IHRL. However, there are three shortcomings to this approach.

First, Article 36 AP1 is notoriously weakly implemented. Only a few states have publicly stated that they conduct regular reviews of new weapons they develop or acquire and there is no international body or forum to oversee the review process. Second, states might argue that if they do not cause any physical effects, cyber-capabilities do not qualify as ‘weapon, means or method of warfare’ and hence fall outside the scope of Article 36 AP1. Third, even when a cyber-capability is not unlawful under IHRL by nature, it could nevertheless be used in a manner incompatible with IHRL. As cyber-capabilities usually exploit specific weaknesses in the enemy’s system, nature and use of

---

177 Article 36 AP1 (emphasis added).
179 William H Boothby, Weapons and the Law of Armed Conflict (Oxford University Press 2016) at 19.5
180 Pilloud and others (n 52) 426.
cyber-capabilities might be identical in some cases. For instance, the Stuxnet code was specifically designed for one specific target, namely the turbines in the targeted nuclear facility. On the other hand, general techniques (e.g., DoS attacks overwhelming servers with requests), could be considered one class of weapons which is not problematic by nature, but only if used in a certain manner. Imagine a DDoS operation that is strictly limited to military devices and has no spill-over effects on the lives of civilians. This operation would most likely not infringe any human rights. However, the very same technology could be used to render all cash machines and online banking tools dysfunctional, hence affecting the right to property. The general method of overwhelming a service or device with requests and hence causing it to be inaccessible might thus make it through a legal review and could still be used in a way that will affect the enjoyment of human rights.

In addition to these challenges, cyber capabilities often need to be constantly modified and updated to respond to changes in the target system. Conducting a new review after every change, however minimal, might be infeasible.\footnote{Gary D Brown and Andrew O Metcalf, ‘Easier Said than Done: Legal Reviews of Cyber Weapons’ (2014) 7 Journal of National Security Law and Policy 115, 128.} However, despite the continuous, iterative nature of the review process,\footnote{Marcos Kotlik, ‘Reviewing Legal Weapons Reviews: Is It Possible to Verify Compliance?’ (EJIL: Talk!, 19 March 2020) <https://www.ejiltalk.org/reviewing-legal-weapons-reviews-is-it-possible-to-verify-compliance/> accessed 20 March 2020; Justin McClelland, ‘The Review of Weapons in Accordance with Article 36 of Additional Protocol I’ (2003) 85 International Review of the Red Cross 397, 413.} such a narrow interpretation of the term new would hardly be reconcilable with the purpose of Art 36 API, which is to prevent the use of certain weapons having unlawful effects.\footnote{This interpretation is based on the second part of Article 31(1) VCLT.} Therefore, it seems reasonable to only conduct a new review if the modification in question substantially alters the weapon’s intended effects or operational performance.\footnote{McClelland (n 183) 404; NATO Cooperative Cyber Defence Centre of Excellence (n 2) 466.} Nevertheless, the constantly evolving nature of cyber capabilities is a general complicating factor in applying Article 36 API.

Consequently, emphasising states’ obligation to consider human rights guarantees when reviewing new weapons, means and methods of warfare might
be useful under very specific circumstances, namely if a state actually has a weapons review procedure and has developed or acquired a cyber-capability which would in all foreseeable use-cases be incompatible with a state’s human rights obligations. Such a situation is not entirely unthinkable, but it will most likely be the exception rather than the rule. Hence, given the generally weak enforcement of Article 36 AP1 and the aforementioned cyber-specific challenges, the utility of this approach in ensuring comprehensive protection for civilians will most likely be very limited.

4.2.2 Martens Clause

The Martens Clause (Article 1(2) AP1) was included in the text of AP1 for situations which might arise after the conclusion of the treaties and without being foreseen by the drafters who could not possibly predict all future technological developments. The provision states that ‘[i]n cases not covered by this Protocol or by other international agreements, civilians and combatants remain under the protection and authority of the principles of international law derived from established custom, from the principles of humanity and from the dictates of public conscience’. In light of the fact that the above-identified gap of protection was caused precisely by such a technological development, the Martens Clause seems to be a likely candidate for filling this gap.

Its reference to ‘established custom’ could be interpreted to include customary IHRL. Nevertheless, to argue that the Martens Clause would allow to simply ‘import’ the substance of IHRL into LOAC without heeding the former’s territorial limits would arguably meet fierce resistance from states

---

186 Note that several states (e.g., Belgium, Germany, The Netherlands, New Zealand, Norway, Sweden, Switzerland, the UK and the US) have publicly declared that they conduct legal reviews of new weapons; Vincent Boulanin and Maaike Verbruggen, ‘SIPRI Compendium on Article 36 Reviews’ (SIPRI 2017) 2 <https://www.sipri.org/publications/2017/sipri-background-papers/sipri-compendium-article-36-reviews> accessed 16 February 2023. Should these states develop or acquire a capability that is exclusively designed to, e.g., disable all online-based ways of receiving information and expressing one’s opinions, this might be considered incompatible with human rights obligations.

187 Pilloud and others (n 52) 39, para 55.

188 Article 1(2) AP1.

which are generally reluctant to accept extraterritorial obligations. Indeed, since international law is based on, _inter alia_, the principle of state consent, one might reasonably argue that the Martens Clause cannot be used to circumvent applicability provisions in IHRL treaties states explicitly agreed to. Given the general disagreement about the Clause’s precise content and its legal effect,\(^{190}\) it seems likely that states and commentators would not easily accept such a far-reaching interpretation of Article 1(2) AP1. Furthermore, some of the human rights protections relevant in the context of cyberoperations (e.g., the right to property) might not be widely accepted as customary law. Hence, they would not form part of ‘established custom’, but at most ‘the laws of humanity’. However, the inherent vagueness of this category further decreases the strength of the argument that the Martens Clause allows to apply IHRL norms to cyberoperations with a nexus to armed conflict.

Yet, the Martens Clause could be useful to encourage and legally ground interpretations of existing LOAC which avoid results that are incompatible with IHRL guarantees. This constitutes a rather soft, IHRL-driven bending of LOAC instead of a robust IHRL implant since IHRL would not be directly applicable, but merely used to interpret existing LOAC. Such an approach could nevertheless be helpful to counteract an unfortunate neglect of IHRL when discussing the regulation of military cyberoperations without physical effects. In sum, the Martens Clause might be helpful in supporting the argument that LOAC should be interpreted in a way that would establish legal protection for civilians from all severely harmful cyberoperations, regardless of the physicality of their effects. However, to argue that IHRL protections apply in any situation of armed conflict because of Article 1(2) AP1’s reference to established custom or the laws of humanity would go too far in the view of this author. Consequently, the Martens Clause cannot fill existing gaps in the legal protection of civilians from cyberoperations without physical effects.

In sum, neither of the two approaches discussed here seem to offer truly promising avenues of combining the substantive protections of IHRL with the territorial reach of LOAC. As has been shown, taking IHRL guarantees into account during weapons reviews is unlikely to have a significant positive impact

on the protection of civilians from cyberoperations without physical effects due to the general nature of Article 36 AP1 reviews and its weak implementation. Consequently, only very few situations, if any, in which a capability would be discarded by states as the result of an IHRL-based weapons review are conceivable. The Martens Clause offers a broader way of ‘folding IHRL into LOAC’. However, this author does not believe that the Clause can be stretched so far as to justify the circumvention of explicit provisions in IHRL treaties limiting their territorial applicability. Hence, Article 1(2) AP1 might be a useful stanchion for argumentative construction when militating in favour of IHRL-informed interpretations of existing LOAC, but it will most likely not be more than that. Consequently, neither Article 36 AP1, nor Article 1(2) AP1 can resolve the dilemma set out at the very beginning of this subsection.

V. CONCLUSION

This paper has critically evaluated a common assumption of the literature regarding military cyberoperations without any reasonably foreseeable physical effects with a nexus to armed conflict. The main argument put forward in this respect is that even if the ‘physical anchoring’ of the law of targeting is undone, substantial conceptual and practical challenges remain. Most notably, the protective potential of the principle of distinction is decreased by the interconnected and complex nature of cyberspace, which might make large segments of the internet and its non-physical infrastructure legitimate targets and severely complicate proportionality assessments. Consequently, there is a risk that if the principles of distinction, proportionality and precaution apply, they will serve as permissive ‘licensing tools’, rather than provide effective protection to civilians.

It was submitted that IHRL’s broader substantive scope as well as its focus on individual rights, transparency and accountability seem to be a better fit for the idiosyncratic and complex effects of cyber-contained operations. Yet, its practical utility is greatly limited in IACs: as long as extraterritorial obligations only arise if a state physically controls a person or territory abroad, most cyberoperations with a nexus to armed conflict will escape the reach of human rights obligations. This paper therefore argued that an effects-based approach to the extraterritorial application of human rights treaties should be discussed more systematically in this context.
Connecting both observations, it was purported that the true gap in protection lies not only in the law of targeting’s focus on violent effects. The travaux préparatoires to AP1 suggest that the law of targeting was only considered relevant to operations against persons and objects outside the physical control of the acting belligerent party. In this sense, it is not only physically, but also territorially anchored. In absence of physical control over territory, non-material values and goods could only be affected through the destruction of certain objects, which is why protection therefrom effectively covered both material and non-material goods and values. The rules of the law of targeting hence did not need to be tailored to the protection of immaterial goods like privacy, immaterial property or free expression. How has this changed? Due to the increased societal importance of cyberspace, a person’s dignity, family life and democratic freedoms are now directly targetable even without physical control over territory. Hence, civilians are at risk of falling into a gap between the law of targeting, which seems inadequate even if applicable, and IHRL or even the law of occupation which might be more adequate but inapplicable in absence of physical control.

In the end, there is no panacea to the issues raised by military cyberoperations without physical effects with a nexus to armed conflict. Some have suggested that new norms are needed to satisfyingly regulate military cyberoperations.\(^191\) However, there seems to be little motivation on the side of states to negotiate a new treaty or similar instrument.\(^192\) Assuming that existing rules of international law will remain the relevant framework for the regulation of military cyberoperations for the foreseeable future, this article suggests that there are theoretical and practical reasons to ‘fight on all fronts’, including IHRL, instead of focusing predominantly on LOAC. Importantly, the observations and arguments put forward in this paper are far from sufficient to


conclude that IHRL will provide better protection than LOAC in all conceivable situations. Instead, the far more limited proposition of this paper is that the role of IHRL regarding military cyberoperations should be analysed more thoroughly and taken into account when discussing how LOAC should respond to the increased use of cyber-based means during armed conflict. More specifically, further research would be needed to assess if and to what extent the utility of IHRL is limited by its focus on state actors when non-state groups are among those mounting cyberoperations. Furthermore, a more detailed investigation of the possibility to derogate from human rights obligations during armed conflict and to impose lawful limitations requires scholarly attention.

With a view to Ukraine, the arguments presented in this article suggest that there is some merit in not only focusing on cyberoperations as war crimes, but also as human rights violations. While the European Court of Human Rights might no longer be available as a forum, an increased focus on human rights by civil society and academia might allow for the condemnation of operations which currently do not qualify as war crimes, based on their impact on the enjoyment of human rights. This might also trigger a debate on how to interpret jurisdictional clauses in human rights treaties with a view to cyber-based conduct, which is what might currently prevent the classification of Russian cyberoperations with effects in Ukraine as actual human rights violations.

More generally, as the ongoing conflict in Ukraine shows, powerful states are taking actions which might turn cyberspace into ‘just another domain of warfare’. Legal scholars should critically evaluate to what extent they might acquiesce to such a transformation when predominantly focusing on the rules on targeting while a body of law is available that more directly protects what is at stake, inter alia, for Ukrainians affected by cyberoperations connected to the Russian invasion: the enjoyment of a life in freedom and dignity, both online and offline.