GENEVA ACADEMY

Académie de droit international humanitaire et de droits humains

Academy of International Humanitarian Law and Human Rights

RESEARCH BRIEF

PROTECTING SOCIETIES: ANCHORING A NEW PROTECTION DIMENSION IN INTERNATIONAL LAW IN TIMES OF INCREASED CYBER THREATS

FEBRUARY 2021 I ROBIN GEISS AND HENNING LAHMANN

THE GENEVA ACADEMY A JOINT CENTER OF

THE GRADUATE INSTITUTE GENEVA

INSTITUT DE HAUTES ÉTUDES INTERNATIONALES ET DU DÉVELOPPEMENT

GRADUATE INSTITUTE OF INTERNATIONAL AND DEVELOPMENT STUDIES

UNIVERSITÉ DE GENÈVE

FACULTY OF LAW

ABSTRACT

Adversarial military cyber operations carried out during armed conflict can affect the functioning of civilian societies in unprecedented ways, challenging the protected reach of international humanitarian law (IHL). In light of this, the article argues for the recognition of new protection needs to shield critical societal processes from cyber threats in conflict situations. Although experts and states generally agree that cyber operations are subject to IHL, the digital transformation has added novel vulnerabilities that do not easily map onto the law's traditional rationale of providing baseline protection against the ramifications of kinetic warfare, such as to minimise death, injury, and destruction among the civilian population. Today's military cyber capabilities have the potential to severely impact essential societal processes across economic, financial, scientific, cultural, and healthcare domains as well as public information spaces. While such consequences may be more diffuse and intangible, in an interconnected world they can affect entire societies and cause systemic disruption on a major scale. Recognising this paradigm shift, the article calls for a more comprehensive understanding of what protection of the civilian population in twenty-first century warfare entails. It submits that certain societal processes and functions must be considered assets so essential as to require legal protection under IHL irrespective of possible physical aspects. In order to meaningfully expand IHL's traditionally narrow focus on objects, kinetic warfare, and physical destruction, the article intends to initiate a discussion about adding the protection of essential societal processes as a new protection dimension to the law of armed conflict.

INTRODUCTION

Since the beginning of the digital transformation of modern societies, the use of adversarial cyber operations with the aim of advancing strategic objectives in situations of armed conflict has been a subject of continuing discussion in academic research as well as among states. The proliferation of evermore sophisticated cyber weapons over the past decade combined with an ever-deeper level of interconnectedness, increasing attack surfaces, and vulnerabilities has added more urgency to the question of how this issue is to be dealt with under international law, in particular the rules of armed conflict. There is general agreement that military cyber operations against the enemy conducted during armed conflict are subject to international humanitarian law (IHL). The fact, however, that these rules were conceived and drafted long before the emergence of offensive cyber technologies raises the question whether the existing legal safeguards are sufficient for future cyber conflicts in regard to the protection of societies that are adversely affected by these new capabilities in novel and hitherto inconceivable ways. IHL, in its modern version, developed in light of the experiences of two world wars, was designed to provide baseline protection against the horrors of kinetic warfare, namely, to avoid and in any event minimise death, injury, and destruction among the civilian population.

This rationale has not lost any of its relevance in the twenty-first century. But in view of today's military cyber capabilities a new, additional dimension of disruptive impacts and resultant legal protection needs is emerging: The impacts military cyber operations can have on the functionality of critical civilian infrastructures and essential societal processes across economic, financial, scientific, cultural, and healthcare domains as well as with regard to public opinion formation and other public sectors. While these impacts may be more diffuse and intangible and more difficult to measure than war casualties or physical destruction caused by kinetic means of war, in an increasingly interconnected world they can affect entire societies and cause systemic disruption and economic loss on a major scale. Traditionally, most such impacts would have been considered as inevitable side-effects of warfare; after all, war by its very nature is inherently and fundamentally disruptive for any society; and clearly, IHL was never meant or designed to respond to all of these disruptions. But in the digital era and in light of the evolution and quality of malicious cyber operations witnessed over the past decade, effects that traditionally would have been considered an inevitable 'inconvenience' and side-effect of war, today can be brought about in a far more targeted, coordinated, and strategic manner and on a very large scale. It is against this background that we propose to re-assess the protective scope of international (humanitarian) law and to discuss what humanitarian baseline protection ought to mean in the twenty-first century.

The present article intends to lay out the problem in order to serve as the basis for a more thorough discussion among stakeholders as to necessary clarifications of existing norms or the development of new frameworks. To this end, the paper first maps the contemporary cyber threat landscape by presenting a number of possible scenarios in which state-led cyber operations, conducted in a situation of armed conflict, interfere with processes that

are essential to the functioning of modern interconnected societies. The subsequent section inquires whether, and to what extent, the existing applicable legal frameworks are sufficient to protect societies from the consequences of future cyber conflict. While the focus will be on IHL, the paper furthermore examines the possible applicability and relevance of international human rights law (IHRL) in situations of armed conflict. Based on these findings, the concluding section suggests possible paths forward that are intended to serve as conversation starters for in-depth discussions with all relevant stakeholders.

MAPPING THE THREAT LANDSCAPE: CYBER INTERFERENCE WITH ESSENTIAL SOCIETAL PROCESSES

Cyber operations in and outside situations of armed conflict can impact the functioning of society in a variety of ways, depending on the cyber tools employed and the affected structures, processes, services, or sectors. To date, the vast majority of such cyber operations has occurred outside the context of armed conflict. But with the rapid increase of such disruptive power projections by way of manipulative cyber operations, often dubbed as hybrid warfare, and a surge in peacetime military cyber operations designed to prepare (future) digital battlefields, the classic divide between peace and armed conflict is increasingly eroding. What is more, contemporary debates about the definition and threshold of an 'attack' or whether data constitutes an object in the sense of IHL, are *pars pro toto* of a much bigger debate as to what is to be considered off-limits and what may lawfully be targeted in twenty-first century cyber warfare. As such these debates reflect ongoing contemplations and underlying strategic interests in the causation of certain societal effects also in times of armed conflict. For some, any such contemplations are simply anathema, but for others they align with a predicted evolution of warfare in the digital age towards blackmail scenarios where essential societal processes are disrupted to achieve strategic ends in the run-up of or in times of armed conflict.[1]

A few conceivable scenarios of such interferences with essential societal processes, loosely based on real-world (peacetime) events and partially ignoring traditional peace/war divides, shall illustrate the issue.

SCENARIO A – DDOS OPERATION AGAINST CRITICAL CIVILIAN AND MILITARY IT INFRASTRUCTURES

Utilizing a large-scale botnet consisting of unwitting personal computers and IoT devices spread across the world, the cyber unit of the armed forces of State A launch a large-scale distributed denial-of-service (DDoS) operation against vast swathes of the civilian and military IT infrastructure of State B. Despite continued efforts to mitigate and redirect the incoming data stream, the adversarial operation lasts for three and a half weeks. No physical damage is registered and no person in State B immediately harmed, but for the duration of the operation a number of essential processes and services, both public and private, cannot be provided. As central sectors of the country's administration are effectively incapacitated, citizens are unable to take care of official matters such as filing for social benefits or applying for ID cards or passports. Mail delivery breaks down and remains severely disrupted for almost two months as a result of the attack. The national stock exchange collapses under the attack so that trading has to be suspended for a couple of days, inflicting considerable financial damage on private enterprises and the state's economy at large. As every larger bank's IT systems are affected, ATMs stop working for almost three weeks.

SCENARIO B – RANSOMWARE ATTACKS IN TIMES OF TENSION

During a period of intensifying political tension between States A and B, the cyber unit of the armed forces of State A deploy a ransomware cryptoworm that exploits a vulnerability in the operating system that is running on the IT systems of the national election commission, the municipal traffic control systems, and the communal waste management facilities. Upon infection, the worm encrypts all data on the affected machines and displays a screen that demands from the authorities of State B to publicly declare that they will meet certain demands made by State A. The breakdown of the systems does not lead to any immediate physical damage, but the parliamentary elections in State B have to be postponed and the constant and widespread outages of traffic lights and the suspension of rubbish collection in major cities spread chaos, uncertainty, and discontent among the civilian population. As the cryptoworm self-propagates automatically, it furthermore affects civilian services and infrastructures using the same operating system in States C and D that are not at all involved in the political conflict between A and B. The government of State B eventually gives in, whereupon the affected systems are decrypted as announced. In a variation to this scenario,

1 Ewan Lawson and Richard Barrons, 'Warfare in the Information Age' (2016) 161 The RUSI Journal 20

the infiltrating worm only appears to be a ransomware attack but is in fact a wiper that encrypts all data without the possibility for reversal, leading to a permanent loss of functionality of the affected systems. This leads to sustained disruptions in the affected processes until the systems' operating software has been successfully reinstalled.

SCENARIO C – CLOUD SERVICES PROVIDER IN THIRD STATE

During an armed conflict between States A and B, a cloud services provider run by a company in State C is affected by a highly targeted wiper attack carried out by the armed forces of State B. In its data centres, the service provider hosts indispensable data for a number of essential societal processes in State A: the public education infrastructure extensively uses the cloud services for important administrative data and teaching material. As a result of the cyber operation, the final exams for all secondary schools in State A have to be postponed indefinitely last minute. The country's largest supermarket company is also almost entirely dependent on the cloud service to manage its dairy and meat supply chains, which causes delays and significant shortages of those products in various regions for over a month. A major research institute uses the cloud service to store auxiliary data necessary to carry out phase 3 trials for a new vaccine that promises to be a remedy for a recently discovered influenza virus, with the result that the research cannot proceed for an indefinite period of time. It is later revealed that the armed forces of State A had contracted the cloud service provider to store the personal records of new recruits.

SCENARIO D – CYBER OPERATIONS AGAINST CRITICAL INFRASTRUCTURES

After months of sporadic armed clashes between the forces of State A and State B, a cyber operation targets the industrial control systems (ICS) of the central power stations supplying the capital and the armed forces' central command headquarters, causing protracted shutdowns of the electrical grid. A second operation hits the municipal water facilities in a number of major cities with the same method, leading to a temporary collapse of the water supply. No immediate deaths or injuries are reported, but public life in the capital and two other cities comes to a standstill for almost a week. The largest hospital in the country's second biggest city has to close for a couple of days after a power outage and a malfunctioning backup generator. The hospital's 800 patients have to be reallocated to other medical facilities in the country, numerous vital surgeries have to be postponed.

SCENARIO E – ATTACKING CORE INTERNET INFRASTRUCTURES

During an armed conflict between States A and B, a cyberattack carried out by the armed forces of State B targets the core internet infrastructures in State A, including the two central internet exchange points and the networks of multiple leading internet service providers, causing a widespread and protracted loss of internet connectivity for large parts of the population, leading to chaos and considerable financial losses. As the smaller, neighbouring State C uses much of the same core infrastructure and is to a large extent dependent on connections to and through State A, public life in State C, which is in no way involved in the conflict between A and B, is also negatively affected. The stock exchange of State C has to shut down for three weeks, and several large hospitals can only operate on a reduced level for ten days, forcing the staff to transfer several patients in critical condition to hospitals in State B.

The above scenarios briefly sketch out currently existing cyber capabilities and possible scenarios, loosely based on elements of past cybersecurity incidents that occurred outside of situations of armed conflict. They exemplify a range of possible threats posed by adversarial cyber operations to the functioning of essential societal processes. The subsequent section looks at the applicable law, with a focus on IHL. It will be inquired whether, and to what extent, the existing legal framework is suitable to protect civil society from the consequences of armed conflict carried out in or through cyberspace. In doing so, it will be assumed that the author of the operation is known. Although the issue of reliably attributing cyber operations remains a problem, it will not be dealt with in this discussion paper. Also, it is not the aim to comprehensively analyse the legality (or illegality) of each of the operations and scenarios described above, but to identify and focus on those kinds of impact that in spite of their gravity could fall (or could too easily be argued to fall) through the cracks of existing legal frameworks.

THE EXISTING LEGAL FRAMEWORK

International humanitarian law is guided by the maxim that 'in any armed conflict, the right of the Parties to the conflict to choose methods or means of warfare is not unlimited'.[2] It thus seeks to alleviate the suffering and

2 Additional Protocol to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of international Armed Conflicts (Protocol I) (8 June 1977, entered into force 7 December 1978) 1125 UNTS 3 art 35. See also already Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land adopted by the Second International Peace Conference (The Hague) (adopted 18 October 1907, entered into

destruction caused by armed conflict, in particular in regard to the protection of the civilian population. This is achieved by the stipulation of a number of foundational principles, namely the principle of humanity (the 'Martens Clause'), the principle of distinction, the principle of proportionality, and the principle of military necessity.[3] Furthermore, it is now generally accepted that international human rights law is applicable alongside and concurrently with IHL in situations of armed conflict,[4] although some of the details regarding the interaction of these regimes remain contentious. The following section examines whether and to what extent the existing rules are suited to protect essential societal processes against adversarial cyber operations in situations of armed conflict.[5]

THE APPLICABILITY OF INTERNATIONAL HUMANITARIAN LAW

The 2015 Report of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE) noted 'the established international principles, including, *where applicable*, the principles of humanity, necessity, proportionality and distinction'.[6] Without directly confirming the applicability of IHL to state conflict in and through cyberspace, the GGE thus affirmed that its guiding rationale is relevant for the legal assessment of state cyber conduct. However, as is well known, the subsequent GGE fifth session failed to produce a consensus report, *inter alia* due to the resistance of some states – Russia and China among them[7] – to include an explicit reference to IHL.[8] At the same time, since then a growing number of states and international organizations have publicly come out to acknowledge that the existing rules of IHL are applicable to cyber operations in principle.[9] This is also the position of the ICRC and the scholarly community, including the authors of this paper.

For IHL to apply to cyber conduct, the operation must be carried out in the context of an armed conflict. An international armed conflict exists when there are hostilities between two or more states.[10] The notion of hostilities implies that the parties to the conflict employ means and methods of warfare, which in principle can be limited to adversarial cyber operations and does not need to also involve the kinetic use of force.[11] Still, to date there have not been any international armed conflicts carried out exclusively via cyber means. The use of cyber tactics as complementing more traditional warfare has

force 26 January 2910) art 22

3 See International Committee of the Red Cross, 'Fundamental Principles of IHL' ‹http://casebook.icrc.org/glossary/fundamental-principles-ihl› accessed 25 January 2021

4 Helen McDermott, 'Application of the International Human Rights Law Framework in Cyber Space' in Dapo Akande, Jaako Kuosmanen, Helen McDermott and Dominic Roser (eds), *Human Rights and 21st Century Challenges: Poverty, Conflict, and the Environment* (Oxford University Press 2020) 197

5 See Helen Duffy, 'Trials and Tribulations: Co-Applicability of IHL and Human Rights in an Age of Adjudication' in Ziv Bohrer, Janina Dill and Helen Duffy (eds), *Law Applicable to Armed Conflict* (Cambridge University Press 2020); Janina Dill, 'Towards a Moral Division of Labour between IHL and IHRL during the Conduct of Hostilities' in Ziv Bohrer, Janina Dill and Helen Duffy (eds), *Law Applicable to Armed Conflict* (Cambridge University Press 2020)

6 UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security 'Report by the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (22 July 2015) UN Doc A/70/174 para 28(d) (emphasis added)

7 Michael N Schmitt, 'Wired Warfare 3.0: Protecting the Civilian Population During Cyber Operations' (2019) 101 International Review of the Red Cross 333, 334

8 Michael N Schmitt, 'France Speaks out on IHL and Cyber Operations: Part I' (*EJIL Talk!*, 30 September 2019) ‹https://www.ejiltalk.org/france-speaks-out-on-ihl-and-cyber-operations-part-i/› accessed 25 January 2021

9 See Government of Australia, 'Non Paper: Case Studies on the Application of International Law in Cyberspace' (2020) ‹https://www.dfat.gov.au/sites/default/files/australias-oewg-non-paper-case-studies-on-the-application-of-international-law-in-cyberspace.pdf› accessed 25 January 2021 7; Ministère des Armées de France, 'Droit International Appliqué Aux Opérations Dans Le Cyberspace' (2019) ‹https://www.defense.gouv.fr/content/download/565896/9750885/file/Droit+international+appliqué+aux+opérations+Cyberespace+-+résumé.pdf› accessed 25 January 202112ff; Roy Schondorf, 'Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations (Israel's position)' (EJIL Talk!, 9 December 2020) ‹https://www.ejiltalk.org/israels-perspective-on-key-legal-and-practical-issues-concerning-the-application-of-international-law-to-cyber-operations/› accessed 25 January 2021; Finish Ministry of Foreign Affairs, 'International Law and Cyberspace: Finland's National Positions' (15 October 2020) ‹https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf/12bbbbde-623b-9f86-b254-07d5af3c6d85?t=1603097522727› accessed 25 January 2021 7; Government of New Zealand, 'The Application of International Law to State Activity in Cyberspace' (1 December 2020) ‹https://dpmc.govt.nz/sites/default/files/2020-12/The%20Application%20of%20International%20Law%20to%20State%20Activity%20in%20Cyberspace.pdf› accessed 25 January 2021 para 25; Dutch Ministry of Foreign Affairs, 'Letter to the Parliament on the International Order in Cyberspace: Appendix: International Law in Cyberspace' (5 July 2019) ‹https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace› accessed 25 January 2021 5; Jeremy Wright, 'Cyber and International Law in the 21st Century' (23 May 2018) ‹https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century› accessed 25 January 2021; Council of the European Union, 'Draft Council conclusions on the Commission and the High Representative of the European Union for Foreign Affairs and Security Policy Joint Communication on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, 11357/12 (21 June 2013) para 6; NATO, 'Wales Summit Declaration' (5 September 2014) ‹https://www.nato.int/cps/en/natohq/official_texts_112964.htm› accessed 25 January 2021 para 72; Bolivia, Chile, Guyana, Peru, and the United States have voiced their support for this position in the Organization of American States, see 'Improving Transparency: International Law and State Cyber Operations: Fourth Report', OAS Doc. CJI/doc 603/20 rev 1 corr 1 (5 March 2020) ‹http://www.oas.org/en/sla/iajc/docs/CJI_doc_603-20_rev1_corr1_eng.pdf› accessed 25 January 2021 para 43

10 See Common art 2 of the *Geneva Conventions, International Committee of the Red Cross, Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field* (12 August 1949, entered into force 21 October 1950) 75 UNTS 31 (First Geneva Convention); *Geneva Convention for the Amelioration of the Condition of the Wounded, Sick and Shipwrecked Members of Armed Forces at Sea* (12 August 1949, entered into force 21 October 1950) 75 UNTS 85 (Second Geneva Convention); *Geneva Convention Relative to the Treatment of Prisoners of War* (12 August 1949, entered into force 21 October 1950) 75 UNTS 135 (Third Geneva Convention); *Geneva Convention Relative to the Protection of Civilian Persons in Time of War* (12 August 1949, entered into force 21 October 1950) 75 UNTS 287 (Fourth Geneva Convention)

11 Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press 2017) (hereinafter Tallinn Manual) rule 82 para 11

been observed, on the other hand, with the first confirmed instance probably being the conflict between Russia and Georgia in the summer of 2008.[12]

In the course of hostilities that fall within the scope of IHL, the parties to the conflict are under the obligation to comply with a number of restricting rules. In the following, these rules will be explained one by one, with a focus on their application to the above outlined scenarios of conceivable cyber warfare.

Legal protection against intangible effects *de lege lata*: subject areas

Healthcare sector

Certain civilian infrastructures and components thereof enjoy special protection under IHL. For one, medical services and infrastructures 'must be respected and protected by the parties to the conflict at all times'.[13] This is especially relevant for the issue of cyber conflict as the health care sector has proven to be particularly vulnerable.[14] As pointed out by the International Group of Experts that drafted the Tallinn Manual, 'respecting' medical services and infrastructures implies a state's obligation to refrain from carrying out operations that impede or prevent medical personnel from performing their medical functions or that otherwise adversely affect the humanitarian functions of medical personnel.[15] This obligation extends to the IT infrastructures necessary to carry out these activities.[16] 'Protecting' means that the state is under a further duty to perform positive measures aimed at ensuring that other actors, such as non-state groups, do not impede medical services and infrastructures, either.[17] The (temporary) breakdown of medical services including the forced postponement of vital surgeries in Scenario D would implicate the obligation to respect medical services and infrastructures. The same conclusion arguably holds true for the disruption of vaccine trials at least if this occurs amid a public health crisis and the vaccine would be an essential remedy, as in Scenario C.

Essential civilian logistical supply chains

Similarly, cyber operations that target objects indispensable to the survival of the civilian population are prohibited. The ICRC's study on customary IHL lists as examples for such objects 'foodstuffs, agricultural areas for the production of foodstuffs, crops, livestock, drinking water installations and supplies, and irrigation works', whereby this enumeration is not to be considered exhaustive.[18] The prohibition laid out in Rule 54 of the ICRC Customary Law Study is particularly useful and potentially pathbreaking in the cyber contest in that it is not limited to attacks or a particular type of operation. Instead, it focuses on certain objects and, given that their rendering useless is explicitly included in the rule, also their functionalities, that are considered of essential importance for the civilian population. This logic and the focus on objects and functionalities that deserve to be prioritized in terms of protection, align with discussions about 'critical cyberinfrastructures', core functionalities, and services that are central to the functioning of a society in the digital era. Therefore, for instance, cyber operations that intrude into and corrupt the functioning of industrial control systems of water treatment facilities would violate this rule. In this context, the prohibition's scope covers not only attempts by cyber means to disrupt the operation of objects indispensable to the survival of the civilian population but also to manipulate it, as happened in 2015 when hackers managed to alter valves to cause a change of the chemical mix at a water treatment facility.[19] However, it must be asked at what point a service or infrastructure reaches the threshold of becoming 'indispensable to the survival' – disrupting the operations of a single grocery store would certainly not suffice; whether the breakdown of meat and dairy supply chains and subsequent shortages of those products for the period of a month, as in Scenario C, would be enough to assume a violation of the rule is still not straightforward. Furthermore, not every important service is 'indispensable' in the sense of Rule 54 of the ICRC Customary Law Study. The suspension of rubbish collection

12 Sarah P White, 'Understanding Cyberwarfare: Lessons from the Russia-Georgia War' (*Modern War Institute*, 20 March 2018) ‹https://mwi.usma.edu/understanding-cyberwarfare-lessons-russia-georgia-war/› accessed 25 January 2021

13 Kubo Mačák, Laurent Gisel and Tilman Rodenhäuser, 'Cyber Attacks against Hospitals and the COVID-19 Pandemic: How Strong Are International Law Protections?' (*Just Security*, 27 March 2020) ‹https://www.justsecurity.org/69407/cyber-attacks-against-hospitals-and-the-covid-19-pandemic-how-strong-are-international-law-protections/› accessed 25 January 2021

14 Laurent Gisel and Tilman Rodenhäuser, 'Cyber Operations and International Humanitarian Law: Five Key Points' (*Humanitarian Law & Policy*, 28 November 2019) ‹https://blogs.icrc.org/law-and-policy/2019/11/28/cyber-operations-ihl-five-key-points/› accessed 25 January 2021

15 Schmitt (n 11) rule 131 para 5

16 ibid rule 132

17 ibid rule 131 para 6

18 Jean-Marie Henckaerts and Louise Doswald-Beck (eds), Customary International Humanitarian Law (Cambridge University Press 2005) rule 54

19 Laurent Gisel and Lukasz Olejnik, 'The Potential Human Cost of Cyber Operations: Starting the Conversation' (*Humanitarian Law & Policy*, 14 November 2018) ‹https://blogs.icrc.org/law-and-policy/2018/11/14/potential-human-cost-cyber-operations/› accessed 25 January 2021

in Scenario B, however inconvenient and seriously disruptive for the normal functioning of modern societies, does at least not immediately threaten the survival of the civilian population as such.

The cultural sector

Finally, in accordance with the 1954 Hague Cultural Property Convention and its Protocols of 1954 and 1999 and the *ratio* of Additional Protocols I and II to the Geneva Conventions, cultural property, that is 'moveable or immoveable property of great importance to the cultural heritage of every people' (Art. 1(a) Cultural Property Convention), enjoys special protection under IHL, including against adversarial cyber operations. Similar to the protection afforded to medical services and infrastructures, the Tallinn Manual contends that states are under an obligation to 'respect and protect' such cultural property.[20] To the extent that it can be considered 'unique' despite merely constituting computational representations in the virtual realm, the concept of 'cultural property' might encompass objects that are not of a physical nature, although this assertion is contentious. Either way, as cultural data can easily be copied, leading to multiple instances of the same artefact, the destruction by cyber means of digital cultural property such as copies of songs or movies will rarely implicate the rule.[21]

Legal protection of other critical infrastructures: the question of 'attack'

The protection under existing IHL of essential societal functions, services, or processes that cannot be subsumed under one of the three categories above in principle depends on the legal qualification of the cyber operation that targets or otherwise affects them. Generally, only operations that can be considered *attacks* trigger a number of legal restraints based on fundamental rules of IHL, namely the principles of distinction, of proportionality, and of precautions in attack.[22] Therefore, it needs to be determined whether and at what threshold cyber operations qualify as attacks. The legal debate among scholars and states surrounding this question has not yet been settled.

According to Article 49(1) Additional Protocol I, "attacks' means acts of violence against the adversary, whether in offence or in defence'. Whether a cyber operation falls within the ambit of this concept therefore depends on the scope of interpretation of 'attack'. It is clear that not every employment of cyber tools during armed conflict will meet the threshold.[23] In this respect, the baseline position virtually all stakeholders can agree on is that any cyber operation that reasonably foreseeably leads to physical damage or destruction of objects, or injury or death of persons, qualifies as an 'attack' within the meaning of Article 49(1) AP I.[24] At the same time, the above scenarios show that most conceivable employments of cyber means in a conflict situation between states will not reach the required level, as explicitly clarified by France in 2019.[25]

The question then becomes whether, and if yes under which circumstances, cyber operations that merely affect the *functionality* of targeted systems or infrastructures may amount to an attack. Here, positions diverge considerably. Although the international group of experts that drafted the Tallinn Manual 2.0 was unable to find a consensus on this issue, the majority held that loss of functionality of a targeted system suffices to qualify as an attack whenever the system needs restoration by replacing (some of) its physical components.[26] A few experts went a step further by regarding the requirement to reinstall the system's operating system or particular data as meeting the 'attack' threshold.[27] Among states, there has not yet crystallized a common viewpoint either. The latter, more expansive view concerning functionality loss and need for setting up a targeted system anew is shared by France.[28] In its deliberation within the framework of the OAS, Chile concurred.[29] Australia, on the other hand, in 2020 merely stated that whenever a cyber operation 'rises to the same threshold as that of a kinetic 'attack under IHL', the rules governing such attacks during armed conflict will apply to those kinds of cyber operations',[30] which seems ambiguous at best as to the exact details of the state's understanding.

20 Schmitt (n 11) rule 142

21 ibid para 4ff

22 International Committee of the Red Cross, 'International Humanitarian Law and Cyber Operations During Armed Conflicts' (*ICRC Position Paper*, 28 November 2019) ‹https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts› accessed 25 January 2021 7

23 Gisel and Olejnik (n 19)

24 See Laurent Gisel, Tilman Rodenhäuser and Knut Dörmann, 'Twenty Years on: International Humanitarian Law and the Protection of Civilians Against the Effects of Cyber Operations During Armed Conflicts' (*International Review of the Red Cross*, September 2020) ‹https://international-review.icrc.org/sites/default/files/reviews-pdf/2020-10/Twenty-years-on-IHL-and-cyber-operations-final-version.pdf› accessed 25 January 2021 26ff

25 Michael N Schmitt, 'France Speaks out on IHL and Cyber Operations: Part II' (*EJIL Talk!*, 1 October 2019) ‹https://www.ejiltalk.org/france-speaks-out-on-ihl-and-cyber-operations-part-ii/› accessed 25 January 2021 (emphasis added)

26 Schmitt (n 11) rule 92 para 10

27 ibid para 11

28 Ministère des Armées de France (n 9) 13

29 Organization of American States (n 9) para 43

30 Government of Australia (n 9) 8

An explicitly restrictive position was more recently taken by Israel. Rejecting the idea that a loss of functionality of a system could ever amount to an attack, it has referred to various practices such as certain types of electronic warfare, psychological warfare, and economic sanctions that have never been considered to be attacks as such, and took a restrictive position stating that 'only when a cyber operation is expected to cause physical damage', can it be qualified as an attack within the ambit of IHL.[31] Such a traditionalist standpoint has resonated with certain scholars, who argue that while many types of cyber operations will never fall within the scope of 'attack', this is entirely in line with the fact that military conduct during armed conflict has always known a considerable number of possible operations that stayed below the attack threshold and were thus 'for good reason ... both permissible and subject to less exacting regulation'.[32] Peru has put forth a similarly narrow interpretation.[33]

The U.S. position zooms in on the aspect of reversibility of the consequences of a cyber operation,[34] which would suggest that certain types of non-kinetic effects might be captured in principle, but not as long as any loss of functionality can still be remedied by reparation or reinstallation. In that sense, the view is marginally less restrictive than Israel's. Other OAS member states have argued for an understanding of 'attack' that is even more expansive than the views of France and Chile. As such, Ecuador and Guatemala hold that any cyber operation that causes a loss of functionality of a system is sufficient for the threshold to me met.[35] Bolivia has asserted that a cyber operation 'could be considered an attack when its objective is to disable a state's basic services', such as 'water, electricity, telecommunications, or the financial system',[36] a position seconded by Guyana.[37]

This considerably more expansive reading of the notion of 'attack' has furthermore prominently been advocated by the ICRC. First, the ICRC has submitted that any military operations with the purpose of rendering an object disabled should be considered attacks. This view is based on the doctrinal argument that otherwise, 'the reference to 'neutralization' in the definition of military objective (Article 52 AP I) would be superfluous if an operation aimed at impairing the functionality of an object (i.e. its neutralization) would not constitute an attack'.[38] The second argument invokes the object and purpose of IHL as a whole, 'which is to ensure the protection of the civilian population and civilian objects against the effects of hostilities'.[39] An overly restrictive interpretation of 'attack' would run counter to this fundamental principle of the laws of armed conflict. This standpoint has consistently been reiterated by representatives of the ICRC.[40]

Once it has been determined that an adversarial cyber operation during armed conflict constitutes an attack, the rules on targeting that aim at protecting civilians and the civilian population become relevant. The cardinal rule is the principle of distinction. While Article 48 I AP I clarifies that it generally applies to all military operations irrespective of the question of 'attack',[41] stipulating that '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', which has customary status,[42] most observers agree that the more specific rules on targeting only constrain militaries in the course of carrying out attacks.[43] These rules are, first and foremost, Article 51(2) AP I, which prohibits the targeting of the civilian population as such and of individual civilians; Article 51(4) AP I, which prohibits indiscriminate attacks; and Article 52 AP I, pursuant to which civilian objects shall not be made the object of attacks.

The upshot of this lack of convergence among states and other actors is that for the time being, the qualification of cyber operations that target essential civilian infrastructures remains nebulous. This uncertainty has potentially wide-reaching consequences for the future of military cyber conflict. Accordingly, under a restrictive interpretation

31 Schondorf (n 9)

32 Gary P Corn, 'The Potential Human Costs of Eschewing Cyber Operations' (*Humanitarian Law & Policy*, 31 May 2019) ‹https://blogs.icrc.org/law-and-policy/2019/05/31/potential-human-costs-eschewing-cyber-operations/› accessed 25 January 2021

33 Organization of American States (n 9) para 43

34 U.S. Department of Defense, 'Law of War Manual' (June 2015) ‹https://dod.defense.gov/Portals/1/Documents/law_war_manual15.pdf› accessed 25 January 2021 para 16.5.1ff

35 Organization of American States (n 9) para 44

36 ibid

37 ibid para 45

38 International Committee of the Red Cross, 'International Humanitarian Law and the Challenges of Contemporary Armed Conflicts' (*ICRC Report*, 31 October 2015) ‹https://www.icrc.org/en/document/international-humanitarian-law-and-challenges-contemporary-armed-conflicts› accessed 25 January 2021 41

39 ibid

40 See most recently Laurent Gisel and Tilman Rodenhäuser, 'Cyber Operations and International Humanitarian Law: Five Key Points' (*Humanitarian Law & Policy*, 28 November 2019) ‹https://blogs.icrc.org/law-and-policy/2019/11/28/cyber-operations-ihl-five-key-points/› accessed 25 January 2021; International Committee of the Red Cross (n 22) 7-8

41 International Committee of the Red Cross (n 38) 42

42 Henckaerts and Doswald-Beck (eds) (n 18) rule 1

43 Robin Geiß and Henning Lahmann, 'Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space' (2012) 45 Israel Law Review 381, 382

requiring physical damage, civilian infrastructures and services as well as other societal functionalities – no matter how essential they might be – would be left legally unprotected against manipulative and damaging cyber operations that do not cause any physical destruction. This creates, in our view, the rather paradoxical situation that while a direct kinetic attack against a civilian bicycle worth 200 dollars is strictly prohibited under IHL, a cyber operation deliberately causing the loss of 200 million dollars or a nation-wide administrative blackout might not, as long as it does not lead to physical damage. All five scenarios introduced at the outset of this paper bear out this dilemma in varying degrees. In none of the outlined scenarios is the 'attack' threshold met beyond doubt. Absent physical damage, the legal assessment of proponents of less restrictive positions revolves around the question whether the targeted systems and critical infrastructures that are obviously essential for the functioning of the affected societies require repair or reinstallation of operation systems or data in the aftermath of the security incidents, as is probably the case in scenarios B and C. Scenarios A and E, on the other hand, render no such measures necessary, so any more traditional understanding of 'attack' would have to concede that the conduct evades the protective scope of humanitarian law, despite the severe fallout.

What is more, a malware that self-propagates and infects systems that control both military and civilian infrastructures by exploiting software vulnerability found in widely used operating systems would violate the principle of distinction only if the initial release of the malware amounted to an attack.[44] In addition, when assessing how problematic such protective gaps could turn out to be in future cyber warfare contexts, it should also be taken into consideration that even when a cyber operation can be qualified as an attack, the inherent interconnectedness of cyber infrastructures poses serious problems for a meaningful and verifiable real-time distinction between civilian and military objects might simply be impossible in many situations.[45] This is because cyber infrastructure used for both civilian and military purposes is a military objective, as argued by the majority in the literature,[46] although the ICRC has maintained the view that 'such a strict interpretation would be a matter of serious concern'.[47]

If one follows the prevalent views, an operation that targets an adversarial state's cyber infrastructure as such, as in Scenario A,[48] would not violate the principle of distinction as it serves a military objective and the country's infrastructures that connect both civilian and military networks are as such dual-use objects. The same holds true for the cloud services provider in Scenario C. Furthermore, this consideration extends to infrastructure that is not itself part of a state's information and communication technologies but depends on them to operate, such as an electricity provider. Thus, an electrical grid that supplies both military and civilian facilities is as such a legitimate target. To be sure, attacks against power plants that serve military infrastructures, for example through air bombardments, have been possible before the digital revolution, but today it is arguably easier to cause protracted power outages by employing cyber means, with potentially catastrophic ramifications for the civilian population in the target state.

The fact that a military cyber operation does not violate the principle of distinction does not in itself render it lawful. It must furthermore adhere to the principle of proportionality pursuant to Article 51(5)(b) AP I, which is part of customary international law and stipulates that incidental loss of civilian life, injury to civilians, damage to civilian objects or a combination thereof is prohibited if it is excessive in relation to the concrete and direct military advantage anticipated.[49] In view of its specific phrasing, however, it has long been contended that the scope of the proportionality analysis is limited to the physical effects of a cyber operation, i.e. death, injury, or damage.[50] Even if one concedes that loss of functionality of a civilian object may reasonably be subsumed under 'damage', a plausible argument not least with regard to the object and purpose of IHL as reflected by the basic principle stated in Article 48 AP I,[51] it is unclear whether merely temporary outage of essential societal services, infrastructures, and processes can be included in the proportionality calculus as long as they do not lead to concrete risks of death, bodily harm, or physical damage to civilian objects.[52] Despite the fact that both direct and indirect effects of an operation are covered,[53] the severe disruption of the civilian population's everyday life in and of itself is thus likely outside the rule's scope of

44 International Committee of the Red Cross (n 22) 5

45 See in detail Geiß and Lahmann (n 43) 384-390

46 Schmitt (11) rule 101

47Laurent Gisel and Lukasz Olejnik, 'The Potential Human Cost of Cyber Operations', ICRC Expert Meeting (2019) ‹https://www.icrc.org/en/document/potential-human-cost-cyber-operations› accessed 25 January 2021 72.

48 Provided the operation can be considered an 'attack'

49 International Committee of the Red Cross (n 22) 6

50 Schmitt (n 7) 347 n 79.

51 Geiß and Lahmann (n 43) 397

52 Schmitt (n 7) 347 n 79.

53 Schmitt (n 11) rule 113 para 6

protection. On the other hand, it must of course be asked whether this can indeed be considered a paradigm shift as such, given that the outbreak of armed conflict has always had considerable ramifications for affected societies whether or not civilians were directly subject to military operations. This principled consideration should serve as the basis for informed consideration of the various issues in the context of cyber warfare, as laid out above.

Article 57 AP I, finally, deals with the third basic principle, precautions in attack. Despite the heading, it has been contended that the rule at least partly applies to military cyber operations that do not amount to attacks in the above sense, as the first paragraph merely states that 'in the conduct of military operations, constant care shall be taken to spare the civilian population, civilians and civilian objects' and thus does not itself refer to the notion of 'attack'.[54] The rule implies that the military commander who is in charge of a cyber operation against an adversary is under the obligation to continuously monitor and take into account the operation's effects on civilians and civilian infrastructures.[55] The more detailed, specific, and arguably more protective provisions of the second paragraph of Article 57 AP I, however, again only apply to attacks. Therefore, the duty for cyber commanders to take all feasible precautions 'to avoid or at least minimize incidental civilian harm'[56] does not come into play as long as the operation remains below the required threshold. If the necessary level of violence is met so that the operation is to be considered an attack, the guiding paradigm of physicality again becomes relevant. Like the principle of proportionality, the rule understands harm as 'incidental loss of civilian life, injury to civilians and damage to civilian objects', which poses the same questions as to the protection of mere functionality of civil societal processes or infrastructures.

INTERNATIONAL HUMAN RIGHTS LAW

Alongside the applicable IHL framework, international human rights law (IHRL), in principle, also provides protections for civilian society during situations of armed conflict. Indeed, in many ways, human rights protections, given their societal anchoring, are better tailored to grasp and address the systemic ramifications of manipulative military cyber operations affecting societal processes. For example, in Scenario B above, the deployment of the ransomware cryptoworm by the armed forces of State A affects the IT systems of the national election commission in State B, which forces the latter to indefinitely postpone its scheduled parliamentary elections. This consequence of the adversarial cyber operation thus *prima facie* implicates the right to vote of the citizens of B pursuant to Article 25(b) International Covenant on Civil and Political Rights (ICCPR). Article 25(c) ICCPR guarantees every citizen the right *and the opportunity* to have access to public service in his country, which might be violated when a protracted DDoS attack makes administrative services unavailable for a considerable amount of time, as in Scenario A. Scenario C conceives a situation in which the students of State A suffer an infringement on their right to education, which is provided in principle by Article 13 International Covenant on Economic, Social and Cultural Rights (ICESCR). The fact that the wiper attack which targets the cloud services provider furthermore disrupts essential vaccine research engages the protective scope of the right to health pursuant to Article 12(1) ICESCR and potentially even the right to life as laid down in Article 6 ICCPR.[57]

However, the application of IHRL to military cyber operations during armed conflict against essential societal processes meets two legal obstacles that have not been resolved entirely to date, at least not on a universal level. For one, the relationship between IHL and IHRL in many ways remains unsettled. Thus far, the debate has mostly focused on the context of the right to life in armed conflict and the right to personal liberty in relation to the detention on the battlefield of persons who belong to irregular non-state armed groups whose legal status under existing IHL is contentious.[58] As exposed by the introduced conflict scenarios, it now becomes apparent that under the conditions of contemporary cyber warfare, the conflicting parties' armed forces gain access to tools that allow for operations against the adversary that potentially implicate the scope of a wholly different array of human rights guarantees. Therefore, the discussion among stakeholders should be expanded accordingly.

The second legal obstacle is the question of the extraterritorial or, for our purposes, 'virtual scope' of existing human rights guarantees. In order for those rights

54 International Committee of the Red Cross (n 38) 42; Schmitt (n 25), arguing that this legal position appears to be shared by France

55 Schmitt (n 11) rule 114 para 4

56 International Committee of the Red Cross (n 22) 6

57 See on this Kubo Mačák, Laurent Gisel and Tilman Rodenhäuser, 'Cyber Attacks against Hospitals and the COVID-19 Pandemic: How Strong Are International Law Protections?' (*Just Security*, 27 March 2020) ‹https://www.justsecurity.org/69407/cyber-attacks-against-hospitals-and-the-covid-19-pandemic-how-strong-are-international-law-protections/› accessed 25 January 2021; Dapo Akande et al, 'The Second Oxford Statement on International Law Protections of the Healthcare Sector During Covid-19: Safeguarding Vaccine Research' (*Opinio Juris*, 11 August 2020) ‹https://opiniojuris.org/2020/08/11/the-second-oxford-statement-on-international-law-protections-of-the-healthcare-sector-during-covid-19-safeguarding-vaccine-research/› accessed 25 January 2021

58 See most recently Duffy (n 5); Dill (n 5)

to be engaged by an adversarial military cyber operation, the acting state must be bound by IHRL vis-à-vis the citizens of the target state. Traditionally, IHRL was principally understood as addressing a special bond between a state and its own citizens and persons located on the state's territory.[59] Over time, this scope was expanded to include individuals within the state's power or effective control.[60] Accordingly, the majority of the group of experts that drafted the Tallinn Manual 2.0 concluded that under international law *de lege lata*, 'physical control over territory or the individual is required before human rights law obligations are triggered'.[61] However, more recently, the UN Human Rights Committee submitted that at least the scope of the right to life pursuant to Article 6 ICCPR comprised 'persons located outside any territory effectively controlled by the State, whose right to life is nonetheless impacted by its military or other activities in a direct and reasonably foreseeable manner'.[62] While this phrasing was clearly geared towards lethal military operations outside of traditional theatres of conflict, such as via armed drone deployment, there is no reason not to apply this reasoning to cyber operations.[63] In legal scholarship, there seems to be a growing consensus as to such an expanded interpretation of IHRL application, including in regard to cyber warfare.[64] At the same time, it must be added that this discussion has been limited to the right to health, although there are no doctrinal reasons not to apply the same consideration to other human rights guarantees, including the ones mentioned above. However, it is more doubtful whether this development already finds the necessary support in state practice and *opinio juris*.[65]

AGENDA FOR DISCUSSION: POSSIBLE PATHS FORWARD

Where does all of that leave us? The analysis has exposed that the existing rules of IHL were originally conceived with an entirely different type of hostilities in mind. Their general scope and underlying assumptions are tailored towards the physical effects of the conduct of hostilities and focused on the mitigation of suffering brought about by physical violence as traditionally understood. It is thus less clear whether they can effectively regulate the full spectrum of modern conflicts involving cyber means and constrain the warring parties, despite the insistence by a number of actors, the ICRC chiefly among them, that this is possible, and indeed inherent in the framework's *raison d'être* to render the rules suitable for any kind of emerging technology.

The possibilities of contemporary military cyber technologies and capabilities pose risks to the functioning of a wide range of essential societal processes not originally envisaged by IHL.[66] Further detrimental consequences of armed conflict – especially the more diffuse ramifications for systemic societal processes and public life – were, at most, an afterthought. In that sense, modern cyber conflict can be considered a paradigm shift, as serious and lasting disruptions of civil society are now not only thinkable but increasingly a reality even without the infliction of any physical damage, as above scenarios demonstrate. In the long run, these developments may come to be seen as a mere starting point to a more fundamental change in warfare. Especially in inter-state constellations, traditional hostilities may increasingly be replaced with blackmail scenarios and manipulative strategies aiming at the economic, financial, and health sectors of a targeted society.[67] With a rapid technological evolution and ever-increasing interdependencies and attack surfaces across all societal domains, in the long run there is a real risk of a gradual undermining if not a reversal of the fundamental understanding that the civilian population must not be targeted in times of armed conflict.

The twentieth-century approach of confining the protective reach of IHL's rules concerning the conduct of hostilities to physical manifestations of violence and damage will leave essential

59 See Samantha Besson, 'Due Diligence and Extraterritorial Human Rights Obligations – Mind the Gap!' (2020) 9/1 ESIL Reflections ‹https://esil-sedi.eu/esil-reflection-due-diligence-and-extraterritorial-human-rights-obligations-mind-the-gap/› accessed 25 January 2021 1

60 UN Human Rights Committee, General Comment No 31 (29 March 2004) CCPR/C/21/Rev.1/Add.13 para 10

61Schmitt (n 11) rule 34 para 9

62 UN Human Rights Committee, General Comment No 36 (30 October 2018) CCPR/C/GC/36 para 63

63 See Mačák, Gisel and Rodenhäuser (n 57)

64 See most recently Marko Milanovic and Michael N Schmitt, 'Cyber Attacks and Cyber (Mis)Information Operations During a Pandemic' (2020) 11 Journal of National Security Law & Policy 247, 261-266.

65 See Daniel Møgster, 'Towards Universality: Activities Impacting the Enjoyment of the Right to Life and the Extraterritorial Application of the ICCPR' (*EJIL Talk!*, 27 November 2018) ‹https://www.ejiltalk.org/towards-universality-activities-impacting-the-enjoyment-of-the-right-to-life-and-the-extraterritorial-application-of-the-iccpr/› accessed 25 January 2021

66 See Schmitt (n 7) 344

67 Konstantin von Hammerstein, 'So können Sie jedes europäische Land in nur 14 Tagen in die Knie zwingen' *Spiegel* (Hamburg 23 May 2020)

aspects of civilian life unprotected and vulnerable to direct attacks in the twenty-first. In our view, contemporary warfare calls for a more comprehensive understanding of what protection of the civilian population entails; an understanding that takes into account the central importance of various societal processes. Interestingly, in the realm of the jus ad bellum, states currently appear to be more readily prepared to include new dimensions of protection that accept non-physical effects on digital and a wide range of societal processes (economic, financial, cultural) as falling within the scope of concepts such as sovereignty, non-intervention, or the use of force. For instance, in its recent position paper, Israel concedes that 'there may be room to further examine whether operations not causing physical damage could also amount to a use of force'. At the same time, it strikingly emphasizes that in the realm of the jus in bello, 'only when a cyber operation is expected to cause physical damage, will it satisfy this element of an attack under LOAC'.[68] In our view, however, and also considering how traditional distinctions between peace and war continue to erode in cyberspace in particular, similar protection needs attach in all of these dimensions. In recent debates regarding Covid-19-related cyber interferences with the health sector, it was interesting to see how IHL's traditional protection focus on hospital protection informed contemporary norm-clarification processes on the level of the jus ad bellum.[69]

Against this backdrop and considering the rapid evolution of military cyber capabilities and resources, we believe that more discussion is needed within the context of IHL as well with regard to economic, financial, or other societal processes – with the aim to potentially anchor a new protection dimension in IHL and indeed in international law more generally. What seems increasingly crucial is not only the civilian population in and of itself, i.e. the natural persons and their physical assets directly at risk from harm, but systemic societal processes writ large whose disruption will entail serious repercussions for the civilian population in its entirety. The challenge ahead, then, is to establish an additional protection dimension in IHL without overstretching this legal regime's protective reach that by its very nature must take into account the military necessities and realities of war.

To be sure, in principle at least, existing rules of IHL – on the basis of a progressive and dynamic interpretation – are not necessarily failing in their effect. As has rightly been stated many times, they already and undoubtedly yield protection in cases where military cyber operations cause effects akin to those of traditional kinetic warfare. However, it is our firm belief that the risks for societies that are increasingly reliant on a functioning cyber ecosystem are too high to tolerate the interpretive grey zones that currently exist. As the law currently stands, and in view of the diverging positions expressed by states and other stakeholders on their interpretation – and for as long as long as IHL's traditional focus on physical damage continues to be seen as the linchpin of all conduct of hostilities rules – interpretations permitting far-reaching operations against societies during armed conflict will remain at least legally defensible. We consider this highly problematic.

After all, such operations could include the paralysation of a country's administration nation-wide, the encryption of tax records of thousands or millions of citizens (even if data was to be seen as an object as long as such operations do not amount to an attack), the breaking down of communal services like water, electricity, or garbage disposal, or the disruption of financial markets or supply chains on a large scale. The fictitious but in our view entirely realistic scenarios analysed in this paper have shed light upon only a limited number of potential ramifications. In view of their scale and gravity – and leaving aside the effects these operations would have on third (neutral) states in a globalized and economically interdependent world – such operations go beyond what in our view could or should be considered permissible psychological warfare, sanctions, or a seizure of property. It is furthermore not clear how operations, such as the encryption of tax records, would contribute to military objectives. Unless genuine blackmailing of the civilian population – beyond propaganda and traditional psychological operations – was to become accepted as a legitimate method of warfare, it would be hard to justify them from a military

68 Schondorf (n 9)

69 See Mačák, Gisel and Rodenhäuser (n 57)

perspective as well.

While we are keenly aware of the inherent limits of IHL's regulative reach – indeed this is a legal regime of last resort aiming to provide baseline rather than perfect or comprehensive protection in times of war – it seems unthinkable to us that in twenty-first century warfare such practices should go entirely unrestrained even when they have nation-wide effects. The primary question therefore is not so much whether such new forms of warfare and the damages they cause can in principle be subsumed under individual rules of IHL, as that is neither here nor there, but whether certain societal processes and functions must be considered assets so essential as to require legal protection under IHL in times of armed conflict. Debates about the notion of 'attack' or whether data could be considered an object, sophisticated and fruitful as they have been, are at risk of missing the bigger picture that what is at stake is a wholly new set of protection needs relating to the disruption of central societal processes and functions. Indeed, contemporary discussions too often remain in a twentieth-century mindset in that they are 'object-focused', i.e. they consider loss of functionality in relation to specific objects that therefore serve as 'intermediaries' for the law to grasp the loss of functionality as a relevant risk or damage. For IHL to fully map onto the twenty-first century's military threat landscape, a more explicit and direct recognition of the protection needs of core societal processes and functions as such will be required. As digitalization continues, and with the increasing merger of cyber capabilities and artificial intelligence, we feel that this will become ever more urgent and evident. After all, in light of cyber operations that could combine technical intrusion and manipulation with disinformation campaigns to undermine a State's financial or administrative systems, the crucial aspect will often not be the loss of functionality of a given object but the disruption of an important societal process or system as such. It is for all of these reasons that we are putting the matter of society protection forward as a new protection dimension in IHL and international law more generally, with a view to initiating a discussion that is focused on contemporary and future protection needs in relation to cyber threats.

To conclude, there are several possible ways ahead. One is to follow the ICRC's approach and to engage in a broad and dynamic interpretation of notions such as 'attack' or 'proportionality' that guide the existing body of law. This important process is currently ongoing. The forthcoming Tallinn Manual 3.0 is likely to give these discussions an additional boost, and it will and should continue as an important element of iterative norm-clarification efforts regarding cyberspace. Still, we remain concerned that in spite of all these welcome endeavours, ultimately too much interpretive ambiguity might remain, not least in view of how much states' and experts' positions on the matter currently diverge. A second possibility is the development and promotion of para- or proto-legal principles for state behaviour in cyberspace during armed conflict in regard to the protection of society that states can voluntary agree on and abide by.[70] Such non-binding norms could conceivably be made part of existing norm-finding and norm-developing processes for responsible state behaviour in the use of information and communication technologies, such as the UN GGE and UN OEWG frameworks, similar to the recommendations laid down in paragraph 13 of the 2015 GGE Report.[71] A third, but at least for the time being unrealistically ambitious approach, would be to suggest the formulation of a new rule. Broadly following the example of Article 54 AP I such a rule could aim to protect core societal processes and functions that are indispensable for a society. Apart from all the difficult line-drawing and threshold discussions that such an approach would inevitably entail, it would arguably also involve a reconceptualization of the protective reach of IHL that includes the protection of society as such. We say 'arguably' because a broad interpretation of the existing concept of the 'civilian population' potentially already comprises the societal processes and functions laid out in this paper. We feel, however, that to meaningfully expand IHL's traditionally narrow focus on objects, kinetic warfare, and physical destruction, a more explicit recognition of the protection of the intangible assets of increasingly digitalized societies is called for. It

70 For a suggestion in this direction see Schmitt (n 7) 343-53

71 See on this United Nations Office of Disarmament Affairs, 'Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of ICT's: a Commentary' (18 March 2020) ‹https://eucyberdirect.eu/content_knowledge_hu/voluntary-non-binding-norms-for-responsible-state-behaviour-in-the-use-of-icts-a-commentary/› accessed 25 January 2021

is to this end that we propose to start a discussion about adding the protection of societies as a new protection dimension to IHL.

THE GENEVA ACADEMY

The Geneva Academy provides post-graduate education, conducts academic legal research and policy studies, and organizes training courses and expert meetings. We concentrate on branches of international law that relate to situations of armed conflict, protracted violence, and human rights protection.

DISRUPTIVE MILITARY TECHNOLOGIES

New (military) technologies are set to revolutionize the ways wars are fought. This research project aims at staying abreast of the various military technology trends; promoting legal and policy debate on new military technologies; and urthering the understanding of the convergent effects of different technological trends shaping the digital battlefield of the future.

The Geneva Academy
of International Humanitarian Law
and Human Rights

Villa Moynier
Rue de Lausanne 120B
CP 1063 - 1211 Geneva 1 - Switzerland
Phone: +41 (22) 908 44 83
Email: info@geneva-academy.ch
www.geneva-academy.ch