International humanitarian law applied to cyber-warfare: precautions, proportionality and the notion of 'attack' under the humanitarian law of armed conflict

Gill, T.D.

DOI
10.4337/9781789904253.00033

Publication date
2021

Document Version
Final published version

Published in
Research Handbook on International Law and Cyberspace

21. International humanitarian law applied to cyber-warfare: precautions, proportionality and the notion of 'attack' under the humanitarian law of armed conflict

Terry D. Gill

1. INTRODUCTION

The applicability of international law to 'cyber-warfare' has received significant attention in recent years. A number of States have presented (semi) official positions on the question of the applicability of international law to cyber-warfare and several noteworthy publications have appeared in which the applicability and application of international law to cyber attacks and other forms of cyber activity have received attention. These include the *Tallinn Manual* on cyber warfare and the follow-up edition including peacetime cyber activity known as *Tallinn 2.0*, along with other publications including the first edition of this Research Handbook and many more too numerous to name.[1] Alongside the applicability to cyber warfare of the *ius ad bellum* governing the permissibility of the use of force and the conditions and modalities relating to its application in response to cyber attacks, the question of the applicability of the *ius in bello*, generally referred to as International Humanitarian Law or the Law of Armed

[1] For examples of State positions on cyber-warfare and the applicability of international law thereto see, Michael N Schmitt (ed), *Tallinn Manual on the Applicability of International Law to Cyber Warfare* (CUP 2013) 2 (hereinafter referred to as Tallinn Manual), citing the national cyber strategies of, *inter alia*, Canada, the Russian Federation, the United Kingdom and the United States. The Netherlands also adopted a position which endorsed the findings of the Advisory Council for International Affairs and the Advisory Committee on Matters of Public International Law Report on Digital Warfare issued in 2011 in which it acknowledged that existing international law, including the law relating to the use of force and international humanitarian law, fully apply to cyber-warfare. See for the joint report of the two bodies AIV/CAVV Report 77/22, *Cyber Warfare*, December 2011 available online http://www.aiv-advies.nl/ContentSuite/upload/aiv/doc/webversie__AIV77CAVV_22_ENG.pdf. For the Dutch Government's response, see http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2012/04/26/cavv-advies-nr-22-bijlage-regeringsreactie-en/cavv-advies-22-bijlage-regeringsreactie-en.pdf. France recently updated its national cyber defence strategy in a publication by the Ministry of Defence, 'International Law Applicable to Operations in Cyberspace' issued in December 2019 see https://opiniojuris.org/2019/09/24/frances-declaration-on-international-law-in-cyberspace-the-law-of-peacetime-cyber-operations-part-i/. Alongside State reactions, a considerable amount of literature has appeared devoting attention to the international legal aspects of cyber-warfare, both in relation to use of force issues and the application of IHL/LOAC These are too numerous to name, but a few examples of some noteworthy publications will serve to illustrate. Among these publications are (2012) 17 *J of Conflict and Security L* devoted wholly to cyber-warfare; Paul Ducheine, Frans Osinga and Joseph Soeters (eds), *Cyber Warfare: Critical Perspectives* (TMC Asser Press 2012); (2013) a series of articles published in 89 *Intl L Studies*; and the publications of the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE), including the aforementioned Tallinn Manual.

Conflict (IHL/LOAC), has also received attention, albeit probably somewhat less on the whole in relation to cyber attacks, than the law governing the use of force. Both aspects are, however, dealt with in the aforementioned *Tallinn Manual*. In this chapter, I will set out some of the main positions put forward in that study and elsewhere relating to the application of IHL to cyber hostilities and offer some personal views in relation to the question to what extent this body of law is relevant and applicable to 'cyber warfare'. In that context, I will devote specific attention to when, under which circumstances and how the rules of humanitarian law relating to the conducting of attacks, with a focus on proportionality, would apply to hostilities carried out wholly or partially in the cyber domain.

This chapter is based on several premises, which however obvious some may seem, need emphasizing. First, that as a matter of law, IHL/LOAC only applies when the conditions relating to the threshold of the existence of an armed conflict have been reached. Secondly, that to date, there has never been a single instance of a 'stand-alone' cyber attack or other act of cyber interference or sabotage, which has come close to meeting that threshold. Thirdly, that the likelihood of such a 'stand -alone' cyber attack reaching that threshold is remote at best.[2] Fourthly, and consequently, that if IHL/LOAC is applicable to 'cyber-warfare', it will most likely be in the context of a 'regular' armed conflict in which cyber operations are conducted alongside traditional 'kinetic' attacks involving the application of IHL/LOAC to the entire spectrum of operations and attacks which are conducted by any party to the conflict. Fifthly and finally, that any armed conflict, irrespective of the means and methods of warfare employed, is subject to the rules and principles of international humanitarian law, and these rules are equally applicable to any party to such a conflict.[3]

This chapter is structured as follows. In the following section, a few considerations will be set out in support of the premises presented above. In the third section, the rules of IHL/LOAC relating to the notion of 'attack', the taking of precautions to spare the civilian population and civilian objects and the duty to conduct such attacks in conformity with the principle of proportionality (as it applies within IHL/LOAC) will be briefly set out. In the fourth section, these rules will be applied in the context of cyber attacks conducted within the context of an armed conflict. In the fifth and final section, a number of conclusions will be presented.

2. WHY AND WHEN HUMANITARIAN LAW WOULD OR WOULD NOT APPLY TO 'CYBER-WARFARE'

The starting point of this explanation of the premises underlying this chapter is that IHL/LOAC is a legal regime which only applies if there is in fact an armed conflict of either an international or non-international character. The qualitative threshold for international armed conflict is provided for in common Article 2 of the Geneva Conventions of 1949 and is restated authoritatively in case law. Although some doubt may arise as to the applicability of all the rules of IHL treaty and customary law in relation to isolated, small-scale incidents involving incidental clashes between the armed forces of two States, it is well established that

---

[2] Thomas Rid, 'Cyber war will not take place' in Ducheine, Osinga and Soeters (n 1) 73.

[3] This follows from the ICJ's statement that international humanitarian law applies to all weapons (past, present, and future weapons) in the context of an armed conflict; see *Legality of the Threat or Use of Nuclear Weapons* (Advisory Opinion) [1996] ICJ Rep 226, para 39.

an international armed conflict exists when there is a conflict between the armed forces of two or more States and/or a total or partial occupation of the territory of a State by another State, irrespective of whether there is armed resistance to such occupation, a situation of declared or factual war, or greater or lesser loss of life and injury, and damage and destruction.[4] In short, any armed clash above the most inconsequential between two or more States results in the existence of an international armed conflict and the applicability of IHL/LOAC to the parties. With regard to non-international armed conflicts, the situation is not as sharply defined, but on the basis of widely accepted criteria set out in the case law of the International Criminal Tribunal for the Former Yugoslavia relating to the requisite degree of organization, intensity and duration, a non-international armed conflict exists when there are armed clashes of an intensity and duration between an organized armed group and a State, or between two or more organized armed groups, which rise above the level of unorganized or sporadic armed violence or civil unrest.[5] If these criteria are met, the rules and principles of IHL/LOAC relating to non-international armed conflict apply to the parties to the conflict, irrespective of how the conflict is characterized by either party. Anything below either of these thresholds is not an armed conflict in the legal sense and IHL/LOAC does not apply as a matter of law, even though either party may elect to apply certain of its rules as a matter of policy.

Although the geographical scope of armed conflict is not the focus of this contribution, it deserves mention that in an international armed conflict (i.e. between two or more States) IHL/LOAC is applicable throughout the territory of any and all States party to the conflict and in international sea and airspace to the extent military operations are conducted there. The territory of third States is inviolable unless one of the parties conducts military operations from the territory of a non-belligerent (neutral) State and that State fails to uphold its duties as a neutral to prevent and put an end to such operations.[6] In non-international armed conflicts, IHL/LOAC applies within the territory of the State in question. It will only apply to the territory of a third State to the extent an armed group (partially) relocates to the territory of a third State and conducts operations from there, without the government of that State taking necessary and adequate measures to prevent or halt such operations being conducted from its territory.[7] The

---

[4] Common art 2 of the Geneva Conventions of 1949, reaffirmed in, inter alia, Jean Pictet (ed), *Commentary to the First Geneva Convention for the Amelioration of the Condition of the Wounded and the Sick in Armed Forces in the Field* (1952) 32. See also *Prosecutor v Dusko Tadić* (Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction) [1995] No ICTY-94-1-A para 70. For discussion whether an international armed conflict results from an isolated low-level armed incident, see, Christopher Greenwood, 'Scope of application of humanitarian law' in Dieter Fleck (ed), *The Handbook of International Humanitarian Law* (OUP 2008) 48.

[5] *Prosecutor v Dusko Tadić* (n 4) para 20; *Prosecutor v. Ramush Haradinaj et.al.* (Judgement) [2008] IT-04-84-T para 60. On the qualification of cyber armed conflict see Arimatsu (Ch 19 of this Handbook).

[6] For the geographic scope of international armed conflict, see e.g. Greenwood (n 4) 59–62; on neutrality law as it applies under the UN Charter, see e.g. Michael Bothe 'The law of neutrality' in Fleck (n 4) 571 *et seq* 582–3.

[7] The normal situation is that non-international armed conflicts occur within the territory of the State in question. In some cases, there is 'spill-over' of a non-international conflict onto the territory of one or more other States whence operations are conducted rising to the level of non-international armed conflict, see, inter alia, Tallinn Manual (n 1) rule 21 (Rule 81 T.2.0) and accompanying commentary 78–9. An example of such a spill-over is the conflict between Iraq supported by an international coalition and the ISIS armed group between 2014 and early 2020 with ISIS operating from its former base of operations in North Syria over the border deep into Iraq at one point controlling a significant portion of

result in both cases is that barring exceptional circumstances, the territory of States not party to the armed conflict is inviolable. In relation to international armed conflicts, this is due to the law of neutrality, alongside rules of general international law relating to State sovereignty and in relation to non-international armed conflicts, due to the latter set of rules arising from principles of State sovereignty and non-intervention, alongside rules and principles arising from the *ius ad bellum*.[8]

Stand-alone cyber attacks have, to date, never met either of these thresholds for the existence of an armed conflict. No example of cyber espionage, interference, intellectual property theft, or even sabotage has until now even approached the threshold of either an international or non-international armed conflict.[9] As serious as cyber espionage, cyber interference and cyber theft and crime are, they are not 'warfare' in anything but a semantic sense. Even when States engage in massive cyber surveillance and espionage, cyber intellectual property theft, cyber interference and cyber non-armed intervention, the lawful responses are to be found in the law relating to law enforcement, retorsion and countermeasures, and not the law relating to the use of force or the humanitarian law of armed conflict. Likewise, cyber terrorism would not automatically trigger the applicability of IHL/LOAC. This would only occur if it resulted in the threshold of either an international or non-international armed conflict, as set out above, being met. There has been, to date, no such example of cyber terrorism, but its occurrence at some point in the future cannot be ruled out. If the necessary conditions relating to the degree of organization, intensity and duration were present, this could result in the applicability of IHL/LOAC, but despite fears of such cyber terrorism, it would seem unlikely that a terrorist group would resort to cyber means instead of the type of terrorist attacks that have been used and are being used by such groups on a regular basis. This is because cyber vulnerabilities are

---

Iraqi territory for a period of several years and with the international coalition supporting Iraq conducting airstrikes against ISIS in both Iraq and in then ISIS controlled areas in North Syria. While opinions differ on whether and at what point an armed conflict between Syria and members of the anti-ISIS coalition may have resulted as a consequence of military action on Syrian territory, there is general agreement that there was a 'spill-over NIAC' in progress between Iraq and the coalition on the one hand and ISIS on the other during that period of time. See e.g. RULAC (Geneva) at http://www.rulac.org/browse/conflicts/non-international-armed-conflicts-in-syria.

[8] The relevance of the principles of sovereignty, non-intervention and the prohibition of the use of force to this question is self-evident. In addition, international law regulating self-defence, while not unanimous in State practice and academic opinion, shows considerable support for the possibility of conducting self-defence in response to armed attack from across an international frontier by a non-State organized armed group if the State from where the attack originated either controls or exercises substantial involvement in the attack, or when a necessity of self-defence otherwise arises often because the State where the armed group is operating is unable or unwilling to prevent such attacks being conducted from its territory. This can lead to a situation where there is an overriding necessity to counter such attacks when other measures are not available or would not suffice to end the ongoing or impending attack. The existence of an armed attack and the lack of feasible alternatives for ending the attack are the key components of the principle of necessity within self-defence, which is the bedrock requirement for its exercise. Only when the State where the operations are conducted from fails to take adequate measures to prevent attacks being mounted from its territory, is there a potential necessity to take action in self-defence. To the extent these operations rise to the level of a non-international armed conflict, humanitarian law relating to such conflicts would become applicable. See, inter alia, Tallinn Manual ibid., 58–9 and 61–6. For further discussion on self-defence in relation to non-State actors see, Terry D Gill and Kinga Tibori-Szabo, 'Twelve key questions on self-defense against non-state actors' (2019) 95 *International Law Studies* 467.

[9] Rid (n 2) 75 et seq.

almost certainly overstated on the one hand and on the other hand, the necessary economic, financial and technical resources to achieve massive societal dislocation on a long-term basis or inflict large-scale casualties by cyber means alone are not readily available to most, if any, terrorist groups.[10]

Neither is it likely, in the event of an armed conflict between States, that massive stand-alone cyber attacks, sometimes referred to as 'cyber Pearl Harbour' scenarios, would be the most likely way in which hostilities were conducted under such circumstances. In the event a large-scale armed offensive were carried out by a State against another State, it would seem illogical that such an attack would be confined to cyber means of warfare. Under such circumstances, the State conducting such an offensive would be most likely to utilize all means of warfare at its disposal. If one decides to conduct all-out warfare for whatever reason, why limit oneself to one weapon alone?[11] Nor is it much more likely that a smaller scale armed attack against a discrete target would be conducted by cyber means alone. The reasons for this are basically twofold. First, such a stand-alone cyber armed attack would not ensure the destruction or effective elimination of the target permanently, or for a prolonged period. If, for example, one wished to take out a particular military capability, platform or critical installation, it would be exceedingly difficult to ensure long-term effective damage, destruction or degrading of the targeted object by cyber means alone. In such a case, cyber techniques of warfare would be much more effective if used in conjunction with traditional 'kinetic' weapons, as was the case in the Israeli attack on the Syrian nuclear reactor in September 2007, when cyber techniques akin to electronic jamming were reportedly used as a means to temporarily neutralize Syrian air defences in order to clear the way for Israeli fighter bombers to attack and destroy the nuclear installation in northern Syria.[12] If, on the other hand, one wished to remain undetected (at least initially) and below the threshold of an armed attack in order to gather intelligence or inflict mere sabotage upon a system, as in the case of the *Stuxnet* sabotage of Iranian nuclear centrifuges, the threshold of an armed attack or of an armed conflict, would not be met. In short, cyber means of surveillance, espionage and sabotage are used regularly by a variety of actors without this being deemed to constitute 'warfare' in either the factual or legal sense.[13]

Consequently, the most likely way in which cyber means and methods of warfare would be used within the context of an armed conflict, aside from intelligence gathering and conducting counter-intelligence and various types of information operations, such as psychological warfare or the influencing of public opinion, would be as an adjunct and assist to attacks conducted by traditional means, as was the case in the aforementioned example of the Israeli airstrike on the Syrian reactor. In such circumstances, cyber operations are essentially another form of electronic warfare, which has been around for a considerable amount of time. The most likely employment would be within the context of operations directed against the adversary's 'sensory and nervous systems', such as degrading command, control and commu-

---

[10] Sean Lawson, 'Beyond cyber-doom: Cyber attack scenarios and the evidence of history' (2012) 10 *J of Information Technology and Politics* 1, 4.

[11] Chinese military strategy is often cited as an example of how cyber methods would likely be used in conjunction with traditional force in the event of any war between the PRC and another State, see Han Bouwmeester, Hans Folmer and Paul Ducheine, 'Cyber security and policy responses' in Ducheine, Osinga and *Soeters* (n 1) 34–7.

[12] Rid (n 2) 84–5. See also Terry D Gill and Paul Ducheine, 'Anticipatory self-defence in the cyber context' (2013) 89 *Intl L Studies* 438, 461–2.

[13] Ibid. 459; Rid (n 2) 85–8.

nications systems, weapons guidance systems, and detection systems like radar systems. This would almost always be conducted alongside more traditional means and methods of warfare, and as such, would be subject to IHL/LOAC rules and principles, including those pertaining to the conducting of 'attacks', whenever such operations amounted to 'acts of violence directed against the adversary, whether in offense or defence',[14] which were reasonably likely to result in physical damage, destruction, death or injury. Hence, while it is quite possible and even likely that cyber-warfare in the real sense of the word will occur at some point, it is most likely to occur in a fairly traditional battle space, both physical and electronic, in which a variety of means and methods of warfare are employed alongside each other, including certain techniques of digital warfare. Because of the resources required to successfully design and employ cyber weapons and the types of operations in which they would be most likely used and most effective, it seems probable that most cyber-warfare in the real sense would occur within the context of international (inter-State) armed conflicts, since most armed groups do not have either the resources, or the type of sophisticated command, control, communications and weapons systems which would make the techniques of cyber-warfare a logical choice of means. If this is a correct surmise, without necessarily ruling out other possible scenarios categorically, then it equally logically follows that whenever such an armed conflict occurs, it will be governed and regulated by the rules and principles of IHL/LOAC which pertain to the conduct of hostilities, including the principle of proportionality in the conducting of 'attacks' which are likely to affect the civilian population, since they apply to all weapons and targeting in any armed conflict. We will therefore now turn to the law which is relevant to such attacks.

3. THE LAW OF ARMED CONFLICT RELATING TO THE CONDUCTING OF ATTACKS

The law relating to the conduct of attacks within IHL/LOAC is primarily contained in Articles 48–58 of the First Additional Protocol to the Geneva Conventions of 1949 (hereinafter referred to as AP I.) While this only applies as treaty law to parties to AP I, which is applicable in international armed conflicts, the customary law relating to the conduct of attacks is substantially similar and binds all States and parties to armed conflict, and is applicable in all armed conflicts whether international or non-international in character.[15] For the sake of simplicity, the relevant provision of AP I will be cited where necessary, when referring to a specific rule or rules.

---

[14] This is the definition of attack under IHL/LOAC as stated in First Additional Protocol to the Geneva Conventions of 1949 (AP I) art 49 and under customary law.

[15] There are at present 174 States Party to AP I. Many, indeed most, of its provisions apply as customary law to non-parties in international armed conflicts and to all parties (both States and non-State armed groups) to non-international armed conflicts, alongside its binding effect upon State Parties to it in international armed conflicts as a matter of treaty law. The provisions of AP I relating to the conduct of attacks which have obtained customary status are reflected in the ICRC customary law study (ICRC CLS), which, notwithstanding certain criticism and shortcomings, has a widely recognized authoritative, but not binding status. For the purposes of this chapter, those rules will be assumed to reflect customary law, since a detailed examination falls outside its scope. The rules in the ICRC CLS relating to attacks are contained in rules 1–24 thereof.

The two main principles of IHL/LOAC in relation to the targeting of persons or objects subject to attack in an armed conflict are distinction and proportionality. These principles act alongside the two main principles of IHL/LOAC which are military necessity and humanity and several other principles, such as the principle of honourable conduct prohibiting perfidy in attacks and the principle of equal application of IHL/LOAC to all parties to the conflict, which form the core structure of this branch of international law.[16] The basic rules relating to the targeting of persons and objects are essentially the following: First, attacks may only be conducted against combatant members of the adversary's forces and military objectives.[17] These include regular members of the armed forces, with the exception of non-combatant military personnel (medical personnel and chaplains), or in non-international conflicts against fighting members of armed groups.[18] In addition, civilians directly participating in hostilities are subject to attack for the duration of their participation, including the period of deployment to and from the place where the attack is conducted.[19] Military objectives are those objects which according to their nature, use, purpose or location make an effective contribution to military operations and whose capture, destruction or neutralization would confer a definite military advantage under the circumstances prevailing at the time an attack is being considered or conducted.[20] Attacks may never be conducted against civilians, civilian objects, protected persons or objects, as such, unless they are directly participating in hostilities or have been converted into military objectives, in which case they lose their protection against attack.[21]

Secondly, in any attack that is likely to affect civilians or civilian objects, the principle of proportionality (as it applies within IHL/LOAC) must be observed. This provides that an attack which is likely to cause excessive civilian casualties or damage or destruction of civilian objects in relation to the concrete and direct anticipated military advantage expected from the attack (viewed a whole) is prohibited.[22] It should be noted that proportionality within IHL/LOAC is only relevant in an attack upon a military objective (including enemy personnel) which is likely to affect the civilian population or civilian objects. An attack which is not likely to affect civilians or civilian objects is not affected by this principle, while an attack deliberately directed against civilians or a civilian object, as such, is strictly prohibited and would constitute a war crime.[23]

---

[16] See e.g. UK Manual on the Law of Armed Conflict (JSP 383 (2004) Chapter 2, 21–6; US Dept. of Defense Law of War Manual 2015 updated December 2016, Chapter II. 50–69.

[17] AP I (n 14) art 49. On distinction in cyberspace see Bannelier (Ch 20 of this Handbook).

[18] Ibid. art 43 and ICRC Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law (26 February 2009) (IG DPH) 32–3.

[19] Ibid., 65.

[20] AP I (n 14) art 52:2.

[21] Ibid., art 51.

[22] Ibid., art 51:5 lit.b.

[23] The applicability of the principle of proportionality to attacks upon military objectives which are likely to affect civilians is clear from the text of art 51:5 lit.b and the scope of the section of AP I in which it appears and is related to protection of the *civilian* population. The weighing of military advantage against likely incidental and collateral effects upon civilians and civilian objects makes this completely clear. Likewise, since proportionality is only relevant in attacks upon military objectives whereby civilians may be affected and attacks against civilians and civilian objects, as such, are prohibited irrespective of any military advantage they might confer, proportionality is only relevant in relation to attacks upon military objectives whereby civilians are likely to be affected. Deliberate attacks upon civilians, as such, are simply prohibited as indiscriminate attacks. Both deliberate attacks upon civilians and dispropor-

Thirdly, constant care must be undertaken to spare the civilian population as far as possible and to prevent, or in any case, minimize loss of civilian life, injury of civilians and damage or destruction of civilian objects resulting from an attack on a military objective. This requires the taking of all feasible precautions when planning and conducting an attack and cancelling or suspending an attack whenever the collateral effects of the attack are likely to be excessive in relation to the concrete and direct military advantage anticipated. This is proportionality in a somewhat different context, namely in choosing the time, method and means of attack least likely to cause excessive collateral injury or damage. The standard here is that of the 'reasonable commander/combatant' acting in good faith and on the basis of information reasonably available at the time the attack is planned or conducted. It also requires an ongoing assessment as to whether the attack remains within the bounds of proportionality at all stages of the attack. Whenever possible, prior warning must be given to civilians likely to be affected, unless this would completely or largely compromise the attack.[24]

Fourthly, means (weapons) and methods of attack which are not or cannot be directed against a specific military objective or objectives or whose effects cannot be limited to military objectives and are consequently indiscriminate are prohibited. Hence means and methods of attack which cannot discriminate between military objectives and civilians and civilian objects are prohibited. Examples of this would be a weapon such as a ballistic missile without a reliable guidance system, such as the Scud missiles used by Iraq in the '*Desert Storm*' campaign, which by their nature could only be indiscriminately directed against geographical areas rather than a specific target, or a means of attack, such as setting a fire in an urban area to force enemy personnel into the open, but which cannot be controlled and is likely to spread indiscriminately affecting civilians and their property along with the intended target.[25]

Fifthly, certain objects such as dams, dykes and nuclear power plants capable of 'releasing dangerous forces' if struck, may only be targeted if they are directly converted into a military function and provide significant support to military operations and no other option is available.[26] The targeting of cultural property is likewise prohibited, except in similar cases and the targeting of objects vital to the survival of the civilian population, or which would cause long-term, widespread and significant harm to the natural environment is prohibited.[27]

Sixthly, weapons or methods of combat which would cause superfluous injury or suffering to enemy combatants are subject to either (far-going) restrictions or are completely banned. The former category includes, inter alia, incendiary weapons and certain types of mines, while the latter includes certain types of munitions (e.g. expanding or flattening bullets) and poisoned, chemical and biological weapons.[28]

---

tionate attacks upon military objectives resulting in excessive (which is not always synonymous with extensive and vice versa) civilian casualties or collateral damage to civilian objects are treated as grave breaches of AP I and constitute war crimes under art 8:2 lit. b (i) and (ii) and (iv) respectively of the Rome Statute of the International Criminal Court.

[24] AP I (n 14) art 57. For the standard of the reasonable commander/combatant, see, inter alia, the Tallinn Manual (n 1) para 13 of the commentary to rule 51 at 163, (rule 113 T.2.0) citing the ruling of the ICTY in the *Prosecutor v Stanislav Galic* (Judgement) [2003] IT-98-29 T para 58.

[25] AP I (n 14) art 51:4, lit. a, b and c respectively.

[26] Ibid., art 56.

[27] Ibid., arts 53, 54 and 55.

[28] Hague Regulations on Land Warfare 1907 art 23(e); ibid., art 35 and specific conventions regulating or banning certain weapons.

Finally, attacks of a perfidious nature (feigning non-combatant or protected status while engaging in attack) are prohibited.[29]

While this summary is not exhaustive, it covers the most important rules relating to the conduct of attacks. In addition, other rules relating to the conduct of hostilities are relevant, such as the duty to refrain from attacks upon protected persons (such as medical personnel) or persons who are *hors de combat* (the wounded, sick, shipwrecked and aircrew bailing out of a stricken aircraft, or who have surrendered at discretion and laid down their arms), so long as they refrain from any hostile act, and the prohibition of denying quarter (not accepting surrender when it is offered or conducting hostilities in a way to allow for no survivors).[30]

4. APPLYING PROPORTIONALITY IN ATTACKS WHICH EMPLOY CYBER WEAPONS

If cyber means and methods of warfare were employed in conducting attacks within the context of an armed conflict, to what extent and how would the law relating to the conduct of attacks set out in the previous section, in particular, the application of the principle of proportionality as it is understood within IHL/LOAC, be relevant? In attempting to answer this question, one should bear in mind a number of considerations. The position taken in the Tallinn Manual and in a number of other publications is that only cyber acts which result in (or are intended to result in) the direct or reasonably foreseeable causation of physical damage, destruction, injury or death are 'attacks' within the context of the law of armed conflict.[31] Consequently, any military operation which does not result in these effects or is intended or reasonably likely to result in such effects (an unsuccessful attack is still an attack), does not involve the principle of proportionality, or any of the other IHL/LOAC rules related to the conduct of attacks. Hence, most military 'information operations', such as psychological warfare, military deception operations designed to mislead the opponent, electronic warfare aimed at jamming or neutralizing electronic communications and weapons guidance or target acquisition systems (unless this was a part of an attack), would fall outside the ambit of 'attack', since they rarely cause such physical effects upon either persons or objects. Likewise the mere gathering of intelligence or conducting of counter-intelligence operations to protect one's own communications and systems, would rarely, if ever, qualify as an 'attack' within the context of the law of armed conflict.[32] That is not to say that there are no relevant rules within IHL/LOAC relating to such operations, but only that these are not related to proportionality and the other rules governing attacks.[33]

---

[29] AP I (n 14) art 37.

[30] First Geneva Convention of 1949 art 24; AP I (n 14) arts 41, 42 and 40 respectively.

[31] Tallinn Manual (n 1) rule 30, with accompanying commentary (rule 92 T.2.0); AP I (n 14) art 49.

[32] For a description and legal analysis of 'information and influence operations', see Blaise Cathcart, 'Legal dimensions of special operations and information operations' in Terry D Gill and Dieter Fleck (eds), *The Handbook of the International Law of Military Operations* (OUP 2015) 449 et seq.

[33] Examples of rules and principles of IHL/LOAC which are not directly related to the conduct of attacks include (but are not limited to) those relating to ruses of war, espionage, misuse of protected, neutral or enemy indicators or status and the duty to take passive precautions (avoidance of locating military objectives in the immediate vicinity of civilians and civilian objects to the maximum extent

Secondly and related to the first point, any operation which only results or is intended to result in mere inconvenience without any foreseeable chance of physical harm or damage, even if this effects the civilian population, equally falls outside the notion of attack, and is not governed by the principle of proportionality. There are two reasons for this: first, because 'attacks' are defined as 'acts of violence' under IHL; and secondly, because proportionality relates to expected collateral civilian death, injury, damage or destruction, which is excessive in relation to the anticipated military advantage from the attack upon a military objective. So if cyber operations resulted in temporary or more prolonged interference with civilian data systems (say e-mail communications or financial transactions), without causing or being intended or likely to cause physical harm (including loss of functionality of the system itself), they would not likely qualify as attacks and proportionality would not be applicable, even if they caused a significant degree of inconvenience and affected daily life to an appreciable extent. Although 'acts of violence' are not limited to the release of physical energy (e.g. chemical weapons are not 'kinetic', but an attack with chemical weapons unquestionably qualifies as an 'attack'), the position taken in the Tallinn Manual is that there must be some physical effects involving damage to, or destruction of, objects, or death or injury of persons for the operation to qualify as an attack, which would make proportionality potentially relevant, and inconvenience, even relatively serious inconvenience, does not normally meet this threshold.[34] On the basis of this interpretation , even if such operations resulted in the destruction or loss of data contained on such systems without resulting in physical harm to persons or damage to objects and without affecting the functionality of the system itself, it would not qualify as an attack in most cases, since data in and of itself has no physical properties.[35] It is arguable, that if the consequences of such destruction of data were reasonably severe, that this could qualify as an act of violence, although this is probably not binding law at present.[36] Moreover if an act were designed to, or likely to result in, the spread of terror or severe mental anguish amongst the civilian population it would, in any case, be prohibited under IHL/LOAC, even if it is not directly related to the notion of proportionality and does not necessarily have any relationship to whether or not data is damaged or destroyed.[37] The destruction of data which could or would likely result in physical effects (e.g. destruction or damage to electronic medical records of patients in a hospital, or the shutdown of a SCADA system controlling a public utility) would in any case qualify as an attack, and depending upon whether it was a side effect of an attack upon a military objective, or simply a deliberate attack upon a civilian system as such, proportionality could enter into the equation. If it were a (foreseeable or unintended) side effect of an attack upon a military objective, proportionality would be relevant and the lawfulness of

feasible). These are dealt with in the abovementioned Tallinn Manual (n 1) in the cyber context in rules 59 and 61–66 with accompanying commentary (rules 121 and 123-127 and rule 89 in T.2.0).

[34] Tallinn Manual (n 1) rule 30, para 12 commentary.

[35] The Group of Experts in the Tallinn Manual ibid. unanimously agreed that whenever an attack directed against data resulted in physical harm or destruction above a *de minimis* level it would qualify as an attack. If this included (possible) harm to civilians and civilian objects, proportionality would be applicable. The majority also agreed that if the functionality of the targeted system were affected to a significant extent, requiring physical replacement of components it could qualify as an attack. See 108–9 for discussion of these issues.

[36] Ibid., rule 38 para 5 of the commentary thereto.

[37] AP I (n 14) art 51:2. For discussion of this in the cyber context see, Tallinn Manual ibid., para 8 commentary to rules 30 and 36 with accompanying commentaries.

the attack would (partly) depend upon whether the collateral effects were excessive in relation to the expected military advantage. If it were simply a direct attack upon a civilian system as such, proportionality would not be relevant to its legality, since any such attack is *ipso facto* illegal to start with.[38] But the notion of attack under IHL/LOAC would, according to this interpretation, not necessarily apply to destruction of or damage to data which did not result or was not intended to result in physical harm or damage of some kind. This would arguably exclude cyber operations which had or were likely to have potentially far-reaching negative consequences for the civilian population (without necessarily resulting in physical harm or damage) from the rules regulating the conduct of attacks, including the principles of distinction and proportionality and the taking of feasible precautions to prevent or mitigate harmful consequences to civilians and civilian life. So, for example, a cyber operation which erased registration of vital statistics such as birth, marriage or death, destroyed property records, permanently rendered bank accounts inaccessible or made it impossible for persons to prove their identity would all be potentially excluded from the rules relating to attack according to this interpretation since none of these would likely result in reasonably foreseeable physical harm, no 'violence' is used in simply erasing data or making it inaccessible and data itself is not an 'object' in the literal sense of Article 49 API. These potentially far-reaching negative consequences have resulted in a number of alternative approaches to the question as to when a cyber operation with potentially harmful non-physical consequences could nevertheless constitute an 'attack' which would render the rules relating to the conduct of attacks applicable. These range from treating data as an 'object' to applying the principle of distinction to military operations with more than negligible, transient or easily reversible negative consequences for individual civilians and the civilian population.[39]

---

[38] See section 3 *supra.*

[39] An early example of the view that an operation directed against civilians constituted an attack was put forward by Knut Dörmann in his paper published in 2004 Applicability of the Additional Protocols to Computer Network Attacks' available at https://www.icrc.org/en/doc/assets/files/other/applicability ofihltocna.pdf. Various authors have proposed taking a teleological approach to art. 49. For example, Heather Harrison Dinniss argues in *Cyber Warfare and the Laws of War* (CUP 2012) 179 *ff*, that while data is not itself an object the information systems on which it is located are and that this would result in cyber operations directed against them constituting an 'attack'; Kubo Macak, 'Military objectives 2.0: The case for interpreting computer data as objects under international humanitarian law' (2015) 48 *Israel Law Review* 55 goes further and argues that data should be treated as an 'object' subjecting all actions directed against it to the targeting rules in IHL. The US (DoD) Law of War Manual seems to take an intermediate position by stating that while attacks involve, in principle, a violent act, harmful consequences above the level of temporary or reversible effects, psychological or information warfare or mere inconvenience could constitute an attack to which distinction and proportionality would apply. See DoD Manual (n 16) Chapter 16, Rules 16.5–16.5.2, 1020–22. In view of the disparity in the views of both States and experts and the lack of conclusive evidence of one position or the other constituting a binding interpretation, it seems fair to say that the issue is at present unresolved. My personal view is close to that put forward in the DoD Manual. I believe that the principle of distinction applies to military operations of any kind with potentially harmful consequences for the civilian population that are more than inconsequential or transient which would make a deliberate CNA on a data system such as those set out in the examples in the text above (vital statistics, property records etc.) an indiscriminate attack which is prohibited under IHL/LOAC. To the extent non-physical harmful effects resulted to civilian data (systems) from an attack on a legitimate military objective, the rules relating to proportionality and precautions in conducting attacks would apply since the consequences result from the attack.

Thirdly, any attack not reasonably likely to cause any harm to or appreciable effects upon civilians or civilian objects falls outside the ambit of proportionality even if it causes or results in extensive damage to military objectives or death or injury to persons subject to attack.[40] Hence, an attack upon a self-contained military data system, such as an insulated military communications, target acquisition, or weapons guidance system, as presumably was the case in relation to the earlier mentioned Israeli attack on the Syrian air defence system in 2007, would not involve any considerations of proportionality, since such systems are normally (highly) insulated from civilian systems and little or no question of likely collateral effects arises. Likewise, if the cyber weapon or technique used in an attack were specifically designed to effect only (certain features of) a specific military target and any collateral effects were likely to only be negligible, proportionality would only enter into the equation if the effects turned out to be appreciable and could have been reasonably foreseen. For example, the Stuxnet virus, although used outside the context of an armed conflict, was such a weapon. Although it apparently subsequently spread to a considerable number of (civilian) computer systems in the region, its effects upon them were virtually non-existent or negligible, since it had been specifically designed to only affect certain components within the Iranian nuclear programme.[41] Had it been used within the context of an armed conflict, the question of its proportionality would scarcely, if at all, have been relevant.

Finally, to the extent an attack upon a military objective were (partially) conducted by cyber means, the rules and principles governing attacks would be relevant to the extent the target had a dual use function, or there was an appreciable chance of collateral effects which would meet the threshold of physical damage or personal injury to civilians or civilian objects. This is perhaps stating the obvious, but there can be no doubt that the principle of proportionality would then apply. This would be the case, irrespective of whether the attack were conducted in conjunction with traditional 'kinetic' weapons, or by cyber means alone. In the former case, the principle would apply to all aspects of the attack, including the cyber component thereof, since an attack has to be viewed as a single act and not chopped into separate segments (e.g. loading, aiming and firing a weapon is all part of a single act once it has been completed.) Hence an attack upon a military objective carried out by a combination of cyber and kinetic means should be assessed as a whole.[42] In the latter case involving a stand-alone cyber attack, proportionality would be applicable whenever and to the extent such an attack on a legitimate target was reasonably likely to result in foreseeable collateral physical effects to civilians and civilian objects including damage or destruction of civilian data systems which could result in physical harm or damage. In principle, there is no difference in terms of assessing the legality of such an attack in terms of proportionality from one which was conducted by traditional kinetic weapons. Consequently, it would be lawful to the extent it did not transgress any of the rules relating to the conduct of attacks, including the principle of proportionality. In short

---

[40] See n 22 and accompanying text *supra.*

[41] Rid (n 2) 84–6. It is likely that in both cases, the cyber weapon (virus, worm, etc) was inserted into the targeted systems (which were hardly likely to be connected to the Internet) by means of a removable drive such as a USB stick.

[42] An attack is seen as commencing once a person or object is endangered (e.g. laying a mine is part of an attack long before its detonation). By analogy, a cyber attack commences once malware is introduced which is reasonably likely to result in physical harm or destruction, even if the effect is delayed or fails to occur, due to detection or malfunction. See Tallinn Manual (n 1) paras 14–9 of the commentary to rule 30 (rule 92 T.2.0).

it would be disproportionate if the collateral effects, whether intended or simply a reasonably foreseeable by-product of the attack, were excessive in relation to the anticipated military advantage, based upon the information reasonably available at the time the attack was being planned and conducted. Moreover, it would also depend upon whether all feasible precautions had been taken before and throughout the attack to limit the effects thereof to the maximum extent possible, and where the situation called for it, the attack had been cancelled or suspended once it was in progress if the situation demanded this. Finally, it could also depend upon whether prior warning had been given to civilians before the attack was undertaken whenever this was possible. Examples of such attacks involving cyber weapons or techniques (either alone or alongside traditional weapons) would be against industrial installations, dual-use objects, such as power plants, or communications systems used for both military and civilian purposes. Provided these rose to the level of an attack as set out above, proportionality would govern such attacks in the same way it governs traditional attacks. There are few, if any differences in this regard.

Nevertheless, as stated in the opening sections of this chapter, there is probably little likelihood of such attacks being conducted by purely cyber means alone, aside from exceptional circumstances, for the reasons stated earlier. Consequently, the assessment of proportionality, will in most cases, likely be no different than if the attack had been wholly conducted by kinetic weapons. In any case, the law is the same irrespective of the (combination of) weapons employed.

5. CONCLUDING REMARKS

The main questions posed in the preceding sections of this chapter were to what extent would attacks within the context of an armed conflict which were conducted by digital means, either on their own, or in conjunction with traditional kinetic force, be likely to qualify as 'attacks' under IHL/LOAC (acts of violence resulting in physical harm to persons or damage to objects) and when and to what extent would this involve the applicability of the rules of IHL/LOAC governing the conduct of attacks, including in particular the principle of proportionality *in bello*? On the basis of the preceding examination and discussion of these questions a number of conclusions can be drawn.

First, IHL/LOAC only applies in the context of an armed conflict and no cyber attack on its own has hitherto qualified as reaching the threshold of an armed conflict. However, on at least one occasion (Israel's attack on a Syrian nuclear facility in 2007), cyber means of warfare were reportedly used in conjunction with kinetic force and this without doubt qualified as an attack which was governed by IHL. Moreover any act which caused or was intended to or was reasonably likely to cause any appreciable danger of physical harm or damage would qualify as an attack, if it were carried out within the context of an armed conflict. This could include attacks conducted by digital means, provided the threshold of an armed conflict had been met and the act fitted into the above-mentioned definition and qualification of an 'attack'.

In that context, it was argued that the most likely scenario in which cyber operations would be used as a means of attack would be in conjunction with traditional kinetic weapons as in the example referred to above and that this is more probable within the context of an international armed conflict than in most armed conflicts of a non-international character. This was primarily because most armed groups have neither the capability of mounting a purely

digital operation qualifying as an attack, nor do most of them have the types of sophisticated command, communications and weapons systems which would be the most likely objects of a digital attack. Moreover, many cyber operations which are likely to be engaged in any kind of armed conflict, such as information operations, surveillance and (counter) intelligence do not qualify as attacks and are not subject to the rules governing attack, including the principle of proportionality. Be that as it may, any act which did amount to an attack would nevertheless be governed by the IHL/LOAC rules regulating attacks, if an armed conflict were in progress, irrespective of whether it was of an international or non-international character.

After setting out the applicable law relating to the conduct of attacks, it was further argued that in view of the above-mentioned considerations, seen in context with the function and purpose of the principle of proportionality, as it applies within IHL/LOAC, that only attacks upon military objectives, whereby it was foreseeable that civilians or civilian objects would be affected, would be governed by the principle of proportionality. Hence attacks upon purely military targets, without any likely appreciable consequences to civilians or civilian objects would fall outside the applicability of proportionality. Likewise in any attack which was directed against purely civilian objects or the civilian population, as such, would be *ipso facto* illegal and no considerations of proportionality would enter into assessing its illegality. Consequently, cyber attacks (either on their own or in conjunction with more traditional weapons) upon insulated military systems and similar military objectives, whereby the possible consequences to civilians or civilian objects were non-existent or negligible and attacks upon civilians and civilian objects, as such, are not subject to proportionality considerations.

This still leaves a fairly wide scope for the applicability of the principle of proportionality to attacks in which cyber weapons or techniques could be used. While, as was discussed, there are some specific considerations relating to how the principle would be applied if cyber entered the equation (such as whether destruction of data effecting the civilian population or whether cyber operations with no physical consequences, but resulting in significant harmful effects on the civilian population qualify as 'attacks' in the context of IHL/LOAC), the principle itself and its basic function along with the conditions relating to whether an attack is carried out in conformity with the principle of proportionality, are not significantly, if at all, different when cyber weapons are employed than if they are not. Hence, proportionality applies in much the same way to cyber attacks conducted within the scope of an armed conflict as to any other type of attack, using any weapon, traditional, or non-traditional.