Israel Law Review **45**(3) 2012, pp 381– 399. © Cambridge University Press and The Faculty of Law, The Hebrew University of Jerusalem, 2012.
doi:10.1017/S0021223712000179

Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space

*Robin Geiß and Henning Lahmann**

While the rules of the jus in bello *are generally operative in cyberspace, it appears to be problematic to apply the fundamental principle of distinction because of the systemic interconnection of military and civilian infrastructure in the cyber realm. In this regard, the application of the accepted legal definition of military objectives will make various components of the civilian cyber infrastructure a legitimate military objective. In order to avoid serious repercussions for the civilian population that might follow from this inherent interconnectedness, different concepts are analysed that could provide potential solutions for a clearer separation of legitimate military targets and protected civilian installations and networks. The approaches discussed range from the exemption of central cyber infrastructure components that serve important civilian functions, to the creation of 'digital safe havens' and possible precautionary obligations regarding the segregation of military and civilian networks. As a solution, the authors propose a dynamic interpretation of the wording 'damage to civilian objects' within the principle of proportionality of Article 51(5)(b) of Additional Protocol I, an interpretation that would comprise the degradation of the functionality of systems that serve important civilian functions.*

Keywords: cyber warfare, principle of distinction, dual-use objects, precautionary obligations, principle of proportionality.

1. Introduction

Cyberspace is opening up a new war-fighting domain: an artificial theatre of war, additional to the natural theatres of land, air, sea and outer space.[1] Today, cyberspace has become hugely important for the military, and there is little doubt that it will only grow in importance in the future. A recent report by the US-China Economic and Security Review Commission concludes that 'the Chinese People's Liberation Army (PLA) has long considered the ability to seize information dominance as prerequisite for achieving victory in future high tech conflicts, but only

*University of Potsdam, robin.geiss@uni-potsdam.de.
The authors would like to thank Yaël Ronen and the anonymous reviewers for their critique and helpful comments.
[1] '[C]yberspace is now as relevant a domain for DoD [Department of Defence] activities as the naturally occurring domains of land, sea, air, and space. There is no exaggerating our dependence on DoD's information networks for command and control of our forces, the intelligence and logistics on which they depend, and the weapons technologies we develop in the field': United States Dept of Defense, 'Quadrennial Defense Review Report' (February 2010, 37), http://www.defense.gov/qdr/.
As far as the Chinese position is concerned, the US-China Economic and Security Review Commission has held that 'PLA [People's Liberation Army] leaders have embraced the idea that successful war fighting is predicated on the ability to exert control over an adversary's information and information systems, often pre-emptively. This goal has effectively created a new strategic and tactical high ground, occupying which has become just as important for controlling the battle space as its geographic equivalent in the physical domain': US-China Economic and Security Review Commission, 'Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage' (7 March 2012, 9), http://www.uscc.gov/RFP/2012/USCC%20Report_Chinese_CapabilitiesforComputer_NetworkOperationsandCyberEspionage.pdf.

recently has it begun to develop the capability to convert this strategic requirement into an operational possibility'.[2]

Against this background, today, there seems to be widespread consensus that 'there is no legal vacuum in cyberspace'.[3] Certainly, as far as the *jus in bello* is concerned, this statement finds support in the Martens Clause, Article 36 of Additional Protocol I[4] and the Advisory Opinion of the International Court of Justice (ICJ) on the Legality of Nuclear Weapons.[5] Against this background, thus far, legal discussions have focused primarily on the question of *when* the laws of war are applicable in relation to military cyber operations.[6] First and foremost, this has been a line-drawing exercise – that is, a threshold debate concerning the question of when military cyber operations rise to the level of an armed conflict or, once there is an armed conflict, whether they qualify as an 'attack' under the laws of war. These are fundamental questions given that only an armed conflict renders applicable the laws of war and given that – at least according to the majority opinion – only an 'attack' in the legal sense of Article 49 of Additional Protocol I is constrained by the principles of distinction and proportionality.[7]

Much less attention, however, has been devoted to the question of *how* these fundamental humanitarian law principles will work out in cyberspace. A recent report of the United Nations Secretary General speaks about 'new and unique challenges' in this regard.[8] The specific technological characteristics and the sheer 'otherness' of cyberspace, compared to the natural theatres of warfare, raise the question whether the application of the established humanitarian legal principles also adequately meets the specific humanitarian concerns of the cyber domain where military and civilian installations appear to be inherently interconnected. In particular, this technological set-up of cyberspace poses a challenge to the application of the principle of distinction.[9] This is the focus of the present contribution.

Whereas it is technically possible to distinguish virtual targets in cyberspace – meaning that a hyper-distinctive attack against a military network is certainly realistic – the application of the

[2] Report of the US-China Economic and Security Review Commission, ibid 15.
[3] Cordula Dröge, 'No Legal Vacuum in Cyberspace' (online interview, 16 August 2011), http://www.icrc.org/eng/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm.
[4] Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (entered into force 7 December 1978) 1125 UNTS 3 (Additional Protocol I).
[5] *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion [1996] ICJ Rep 226.
[6] See Michael N Schmitt, 'Cyber Operations and the Jus in Bello' (2011) 41 Israel Yearbook on Human Rights 113; Michael N Schmitt, 'Wired Warfare: Computer Network Attack and Jus in Bello' (2002) 84 International Review of the Red Cross 365; Knut Dörmann, 'Applicability of the Additional Protocols to Computer Network Attacks' (International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, Stockholm, September 2004), http://www.icrc.org/eng/assets/files/other/applicabilityofihltocna.pdf; Jenny Döge, 'Cyber-Warfare: Challenges for the Applicability of the Traditional Laws of War Regime' (2010) 48 Archiv des Völkerrechts 486.
[7] Robin Geiß, 'The Conduct of Hostilities in and via Cyberspace', ASIL Proceedings 104th Annual Meeting, 2010; Schmitt, 'Wired Warfare' (n 6) 365.
[8] Report of the Secretary-General, Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc A/66/152, December 2011, 19.
[9] cf Jakob Kellenberger, 'International Humanitarian Law and New Weapon Technologies' (Keynote address, 34th Round Table on Current Issues of International Humanitarian Law, San Remo, 8–10 September 2011), http://www.icrc.org/eng/resources/documents/statement/new-weapon-technologies-statement-2011-09-08.htm.

accepted legal definition of military objectives in the interconnected cyber domain will render basically every cyber installation a legitimate military objective. In cyberspace, every component of the cyber infrastructure is a dual-use object. After all, by and large the military uses the very same cyber infrastructure that is used for civilian purposes.[10] And, as is well known, all objects which by their use or intended future use make an effective contribution to military action legally qualify as legitimate military targets, and therefore may be lawfully attacked in the course of an armed conflict.[11] Evidently, this could have far reaching repercussions on the civilian population. Nevertheless, the problem has hardly been addressed at all that, because of the systemic technological set-up of cyberspace in times of an armed conflict, basically every cyber installation – possibly even cyberspace as such – potentially qualifies as a military objective.[12]

Against this background, our analysis proceeds in three parts. First, we will show that the distinction between military and civilian objects in cyberspace, because of the interconnectedness of civilian and military cyber infrastructure, is largely impossible on the basis of the established legal definition of military objectives (below Section 2). Of course, 'dual use' is not a problem exclusive to cyberspace.[13] However, as we will show, the systemic technological set-up of cyberspace, the inherent interconnectedness of civilian and military systems, brings this issue to the fore in unprecedented ways. In essence, the entire cyber infrastructure (that is, computers, servers and cables) is a dual-use object and therefore could be qualified as a legitimate military objective in times of armed conflict. In terms of civilian protection and in view of increasingly cyber-reliant societies, this is a highly problematic conclusion. Therefore, the second part of the analysis (below Section 3) is devoted to potential solutions for a clearer separation of legitimate military targets and protected civilian installations and networks. The approaches discussed range from the exemption of central cyber infrastructure components that serve important civilian functions to the creation of 'digital safe havens' *de lege ferenda* and possible precautionary obligations regarding the segregation of military and civilian networks *de lege lata* on the basis of Article 58 of Additional Protocol I. Finally, in Section 4 we turn to the principle of proportionality which leaves states with a greater margin of flexibility than the more rigid approaches discussed in Section 2 and therefore, at least for the time being, appears to be the most realistic and viable way of mitigating the repercussions for the civilian population.

[10] Eric Talbot Jensen, 'Cyber Warfare and Precautions Against the Effects of Attacks' (2010) 88 Texas Law Review 1522, 1542.

[11] Additional Protocol I (n 4) art 52(2). Of course, the definition contained in art 52(2) of Additional Protocol I is two-pronged in that it not only requires that an object's use would make an effective contribution to military actions but that simultaneously the object's destruction, in the circumstances ruling at the time, would also offer a definite military advantage. However, in reality this second tier has rarely worked as an effective constraint given that typically the destruction of any object which makes an effective contribution to military action also offers a discernible military advantage.

[12] But cf Kellenberger (n 9).

[13] See Henry Shue and David Wippmann, 'Limiting Attacks on Dual-Use Facilities Performing Indispensable Civilian Functions' (2002) 35 Cornell International Law Journal 559.

2. APPLYING THE PRINCIPLE OF DISTINCTION IN AN INTERCONNECTED DOMAIN: THE SYSTEMIC DUAL NATURE OF THE CYBER INFRASTRUCTURE

Where the means and methods of cyber warfare are aimed at traditional military objectives in the 'physical world', and where they result in the same 'real world' effects as would conventional weapons, there appears to be no significant controversy as to the application of the principle of distinction.[14] Whether a given military objective is attacked via cyberspace or via the air by a drone or fighter plane, for the purposes of international humanitarian law, essentially makes no difference. Thus, if a physical object like a military communications centre or an electricity plant is to be attacked and physically destroyed by means of a military cyber operation, the attacking state would first of all be obliged to establish whether the communication centre or, more problematically, the electric power plant in question qualifies as a legitimate military target. Only after having assessed the proportionality of the envisaged attack, and after having taken all required precautions, may the attack lawfully be carried out.[15]

Yet, with the ever increasing military importance of cyberspace, future armed conflicts involving high-tech parties will not only see the use of cyberspace as a medium to direct attacks against physical objects such as power plants or military communication centres. Increasingly, components of the cyberspace infrastructure will become strategic targets in and of themselves.[16] The more important cyberspace becomes for military operations, the greater the strategic interest to degrade an enemy's capacity to use this domain for strategic purposes. Thus, the US Quadrennial Defence Review Report emphasises that 'in the 21st century, modern armed forces simply cannot conduct high-tempo, effective operations without resilient, reliable information and communication networks and assured access to cyberspace'.[17]

Consequently, military strategists appear to have no doubts that controlling cyberspace will become as important a strategic goal for the military as obtaining control over airspace or the sea has been in traditional conflicts.[18] This will logically involve attempts to degrade an enemy's cyber capacities by destroying or manipulating the enemy's cyber assets, infrastructure and key communication nodes.[19] It is no secret that already now the military of various states are preparing a potential future cyber battlefield by way of pre-implanting concealed codes and software tools in various strategically relevant places, as well as by manipulating hardware components along the supply chain.[20] Thus, the question of which networks and components of the cyber

[14] cf Dröge (n 3).
[15] Schmitt, 'Wired Warfare' (n 6) 365.
[16] cf Report of the Secretary-General (n 8) 10.
[17] Quadrennial Defense Review Report (n 1) 37.
[18] cf Report of the US-China Economic and Security Review Commission (n 1).
[19] ibid.
[20] 'By providing counterfeit hardware that already contains the Trojanized access built into the firmware or software, a foreign intelligence service or similarly sophisticated attacker has a greater chance of successfully penetrating these downstream supply chains': Report of the US-China Economic and Security Review Commission (n 1) 11 ff.

infrastructure will qualify as legitimate military objectives gains importance, especially for increasingly cyber-reliant societies, and it is this question to which we now turn.

A sophisticated military cyber attack in the year 2012 has little in common with the 'old-fashioned' computer virus that, like the so-called 'I-love-you-virus' in the year 2000, is hidden in an email and sent from one computer to another.[21] The possibilities of a military hacker are vastly different and portentous. Thus, the herder of a botnet,[22] for example, may utilise thousands or even millions of civilian systems in various countries to generate computer power and to carry out large-scale denial-of-service attacks. Alternatively, a sophisticated military cyber attack could consist of bits and pieces of fragmented malware codes that lay dormant for weeks, months or even years in various systems all over the world and that, triggered by a certain command or event, such as troop mobilisation in an enemy country, are brought together in a predetermined target where the malware unfolds its destructive or manipulative function.[23] Until it does, the codes used for such an operation are typically not recognisable as in any way being malicious. In any case, cyber operations need not even rely on 'malicious' codes or worms. A cyber operation may simply rely on the right code – for example, the standard code for opening a valve in a power plant – but activate it at the wrong time.

If the accepted definition of military objectives contained in Article 52(2) of Additional Protocol I is applied in this context,[24] a wide range of cyber assets that are principally civilian in nature – for example, all the civilian systems unknowingly involved in a botnet – would qualify as legitimate military objectives. They all make an effective contribution to military action by virtue of the way in which they are used and their destruction or neutralisation would offer a definite military advantage in accordance with Article 52(2) of Additional Protocol I.

What is more, (military) codes travelling in cyberspace are split up into various data packages, all of which may travel via different (civilian) channels and typically traverse various civilian systems when travelling through cyberspace. Thus, even in a single cyber attack, a wide range of physical cyber infrastructures – namely servers, routers, cables or satellites, as well as

[21] Sandro Gaycken, *Cyberwar – Das Wettrüsten hat längst begonnen, Vom digitalen Angriff zum realen Ausnahmezustand* (Goldmann 2012).

[22] A computer that has been turned into a so-called 'bot' can perform automated or remote-controlled tasks without the owner/user knowing it: http://www.microsoft.com/security/resources/botnet-whatis.aspx. See also Ralf Hund, Matthias Hamann and Thorsten Holz, 'Towards Next-Generation Botnets' (4th European Conference on Computer Network Defense (EC2ND 08)), http://www.ei.rub.de/media/emma/veroeffentlichungen/2010/08/05/rambot-ec2nd08.pdf.

[23] The recent report of the US-China Economic and Security Review Commission cites the authors of the Peoples Liberation Army publication, 'Information Confrontation Theory', as stating that 'information confrontation forces can potentially plant malicious software in enemy weapons systems that will remain dormant until they are employed; or pre-place malware on enemy information systems that will only activate at a preset time to destroy an enemy's C2 network or those circuits that control operation of railroads and military air routes, or divert trains to wrong routes to cause traffic jams': Report of the US-China Economic and Security Review Commission (n 1) 26, 27, citing Wang Zhengde, Yang Shisong and Zhou Lin (eds), *Xinxi Duikang Lilun* (PLA Information Engineering University/Military Science Publishing House 2007) 12.

[24] 'It is agreed that this definition has acquired the status of customary international law notwithstanding continuing controversy over its interpretation': Jean-Marie Henckaerts and Louise Doswald-Beck (eds), *Customary International Humanitarian Law, vol I: Rules* (International Committee of the Red Cross and Cambridge University Press 2009) (ICRC Study) rule 8.

software – are used to make effective contributions to military action and would thus qualify as legitimate military targets. For example, it is estimated that approximately 98 per cent of US government communications use civilian-owned and -operated networks.[25]

The problem of reliance by the military on civilian systems and infrastructure is further exacerbated by the fact that, under the ambiguous 'purpose criterion' of Article 52(2) of Additional Protocol I, an object's intended future use for military action suffices to render an object a military target.[26] As the commentary to the 2009 Air and Missile Warfare Manual explains, 'the purpose criterion recognizes that an attacker need not wait until a [civilian] object is actually used for military ends before being allowed to attack it as a military objective'.[27] As Dinstein has put it, purpose is predicated on intentions known to guide the adversary.[28] Establishing an enemy's intentions, therefore, is crucial for the application of the purpose criterion. This determination typically hinges on available intelligence. Where uncertainty remains, Article 52(3) provides that in case of doubt – as far as objects normally dedicated to civilian purposes are concerned – the objects in question shall be presumed not to be so used. This latter caveat, however, has not acquired the status of customary law and, in any case, the civilian cyber infrastructure hardly qualifies as an object 'normally dedicated to civilian purposes' given that it is regularly used by the military. Where Article 52(3) is inapplicable, it is not clearly established what degree of certainty or proof is required to establish an enemy's intentions regarding the future use of an object.[29] In the case of cyber infrastructure, however, given that the components of the civilian and military cyber infrastructure are systemically intertwined – in fact, typically it is one and the same infrastructure that is being used – it is clear from the outset of an armed conflict in which the parties employ means of cyber warfare that significant parts of the civilian cyber infrastructure will be used to make an effective contribution to military action. What is unclear, of course, is which components exactly will be used for military purposes. In the cyber realm, however, this has less to do with the unclear intentions of the adversary rather than the functionality of cyberspace as such. In the cyber domain it is typically unclear – including to the author of a cyber operation – which ways his data packages will take in order to arrive at their intended target. In any case, in a future cyber conflict there will be thousands and millions of data packages going in all directions. Because of the systemic interconnectedness of cyberspace, it will hardly ever be possible to prove or to anticipate with any degree of certainty at which millisecond which components of the cyber infrastructure are or will be used for a particular military

[25] Jensen (n 10) 1542.
[26] Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (International Committee of the Red Cross, Martinus Nijhoff 1987) (ICRC Commentary) 2022; Ian Henderson, *The Contemporary Law of Targeting: Military Objectives, Proportionality and Precautions in Attack under Additional Protocol I* (Martinus Nijhoff 2002) 84.
[27] Program on Humanitarian Policy and Conflict Research, 'Commentary on the HPCR Manual on International Law Applicable to Air and Missile Warfare' (version 2.1, March 2010, 107), http://ihlresearch.org/amw/Commentary%20on%20the%20HPCR%20Manual.pdf.
[28] Yoram Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict* (2nd edn, Cambridge University Press 2010) 99–100.
[29] Stefan Oeter, 'Methods and Means of Combat' in Dieter Fleck (ed), *The Handbook of International Humanitarian Law* (Oxford University Press 2008) 81–180.

operation. While we are much in favour of the argument that in view of such uncertainty the presumption should always be in favour of protected (that is, civilian) status, we remain doubtful that such a restrictive approach would find acceptance in state practice, especially if in a future armed conflict the overall strategic aim is to degrade the enemy's cyber capacities.

Of course, an object's current or intended future use in and of itself does not suffice to qualify an object as a legitimate military objective. Article 52(2) of Additional Protocol I requires a two-pronged test; this means that, in addition to the establishment of one of the objective criteria of nature, location, purpose or use, it also needs to be shown that an object's 'destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage'. Notwithstanding, when assessing whether a given object qualifies as a military objective, the emphasis usually lies only on the first part of the definition.[30] Thus, the commentary to the Air and Missile Warfare Manual provides that '[i]n practical terms, compliance with the first criterion will generally result in the advantage required of the second'.[31] In line with this assumption the Commentary states:[32]

> The civilian character of an object can be lost through location, purpose or use. … [A] residence is a civilian object, but becomes a military objective if used to billet troops. Finally, a civilian ocean liner being fitted for intended future use as a military troop transport qualifies as a military objective by purpose.

The problem with such a sweeping conclusion is that it neglects the second part of the definition contained in Article 52(2).

Conversely, to some authors this second part of the definition, by adding a criterion of 'situational relevance', constitutes a significant constraint on the scope of military objectives.[33] While this approach better adheres to the two-pronged structure of Article 52, it is not without problems either. The difficulty is that it is unclear how far the first and the second tests are different from one another. In fact, it seems rather difficult to come up with clear-cut examples where an object is used or intended to be used to make an effective contribution to military action without its destruction offering a definite military advantage to the enemy. The example provided by Shue and Wippmann is that of 'a heavy bridge that would enable tanks to cross into a combat area on the other side of a river' and which would therefore 'generally qualify as a military objective under the first part of the [definition]'. However, according to the authors, 'if in fact no combat is occurring or is likely to occur in the area to which the bridge leads', its destruction – because of a lack of 'situational relevance' – would not offer a definite military advantage and could therefore not be lawfully destroyed.[34]

The problem with this example is that it conflates the first and the second parts of the definition contained in Article 52(2). Because if indeed there is 'no combat occurring or likely to

[30] See eg Dinstein (n 28) 94.
[31] Commentary on the HPCR Manual (n 27) 49.
[32] ibid 32.
[33] Shue and Wippmann (n 13) 561.
[34] ibid.

occur in the area to which the bridge leads', the bridge would not be making an effective contribution to military action in the first place, thereby failing to fulfil even the first part of the definition. The splitting up of the two-pronged test in Article 52(2) into an abstract test (first part) and a concrete test of situational relevance (second part) does not seem to work because the determination of whether an object like a bridge makes an effective contribution to military action (first part) necessarily needs to take into consideration the concrete circumstances. Otherwise a bridge is just a bridge, a civilian object without any military relevance. If Shue and Wippmann were correct, a tank – just like the bridge in their example – that is not currently in use and not likely to be used in the near future would not fulfil the test of 'situational relevance' and would therefore not qualify as a military objective. Such a narrow reading of Article 52(2), while it is a rare attempt to make sense of the two-pronged test contained therein, is unlikely to find acceptance in state practice. Typically, already the first part of the definition, in line with the convoluted wording of the provision, is interpreted to consider aspects of situational relevance, thereby depriving the second part of the test largely of any autonomous meaning.[35]

Because of the technological features of cyberspace, however, it could be possible to come up with examples where the second part of the test is of autonomous relevance. Cyberspace is largely resilient, meaning that if certain communication channels are obstructed or destroyed, the communication flow will simply find another way, and in the interconnected domain of cyberspace there are always various alternatives. Against this background it could be argued that even if the civilian cyber infrastructure, by way of its use or intended future use, makes an effective contribution to military action, its destruction would still not offer a definite military advantage because the destruction or neutralisation of such infrastructure would not significantly hamper the enemy's ability to conduct cyber operations. Of course, no one would argue that the destruction of military barracks does not offer a military advantage simply because the enemy has various other military barracks at its disposal. Cyberspace would allow a different conclusion only if its resilience was such that the destruction or neutralisation of certain infrastructure components would be without any effect whatsoever. This, however, does not appear to be the case. While it may not be possible to shut down the internet in its entirety, degrading the enemy's possibilities to conduct cyber operations is technically possible and will indeed be an overall strategic aim in any future cyber conflict.[36] Therefore, on the basis of the traditional definition of military objectives, one does not even need to go as far as to invoke the controversial approach of qualifying all so-called (economic) 'war sustaining' objects[37] as military objectives;

[35] Dinstein (n 28) 90–91. For example, Dinstein asserts that deserted military barracks remain a military objective and thereby implicitly discards the situational relevance criterion suggested by Shue and Wippmann (n 13) 94.
[36] Report of the US-China Economic and Security Review Commission (n 1) 42–43. See also Northrop Grumman, 'Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation' (Report prepared for the US-China Economic and Security Review Commission, 9 October 2009, 23), http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf.
[37] ibid 110.

it will be possible to qualify a wide range of cyber infrastructure as legitimate military objectives.

Of course, in theory every civilian object in the 'physical world' could also fall within the definition contained in Article 52(2) of Additional Protocol I. Theoretically, every object is a so-called 'dual-use object' on the basis of contemporary international humanitarian law.[38] De facto, however, most civilian objects in the real world simply have no significant military potential and therefore will never be used in a militarily conducive way. This is one aspect in which the cyber domain appears to be fundamentally different. Each and every bit of memory capacity or computer power, wherever it resides, has military potential at all times. This is the reason why civilian and military systems are inherently interconnected. There simply is no difference between a military and a civilian computer; any computer and basically any part of the larger cyber infrastructure can be used to serve the military and the civilian constituency either interchangeably or simultaneously.

Indeed, in the cyber domain such 'dual use' will typically occur simultaneously. Thus, 99 per cent of a server's capacity may be used exclusively to carry out important civilian functions, while 1 per cent, or even only 0.1 per cent, of its capacity may simultaneously be used for military communications and other military purposes. The issue of such simultaneous use – albeit not a problem exclusive to cyberspace, as any electricity plant in times of armed conflict may serve military and civilian purposes simultaneously – as far as can be seen has only rarely been discussed. Notwithstanding, the general view appears to be that *any* military use, however minimal, would render a civilian object a military objective.[39] It follows that in a future 'cyber war' the established definition of military objectives, despite striking an accepted balance between military needs for flexibility and civilian protection in traditional armed conflicts, could render basically every component of the cyber infrastructure a legitimate military objective.

This is not only because of the inherent interconnectedness of cyberspace but also the artificiality of the cyber domain. In a naturally occurring theatre of war like the air, a military fighter jet uses the airspace to travel, but only the aircraft will qualify as a military objective. In the cyber domain, given that it is a man-made domain which ultimately consists of various physical components (of course, in addition to various software components which, however, cannot function without an underlying hardware infrastructure), the focus is not on the travelling malware – malicious codes, as stated above, are typically indistinguishable from other codes and hence impossible to detect – but rather primarily on the physical infrastructure that is used to execute such a cyber operation. These infrastructure components, however, are typically civilian by nature and serve primarily important civilian functions. Thus, even though technically cyberspace would seem to allow for a high degree of precision and, in fact, hyper-distinctive attacks against specific

[38] ibid 108: 'Any civilian object may become a military objective through use, including those entitled to specific protection but abused by a Belligerent Party through military use. Even objects entitled to specific protection, such as medical units or cultural property can become military objectives if so used.' See also Shue and Wippmann (n 13) 565.

[39] Dinstein (n 28) 141.

military installations – Stuxnet being exemplary for such specificity[40] – legally speaking, on the basis of the contemporary definition of military objectives, a country's entire cyber infrastructure could potentially be qualified as a military objective once it engages in an armed conflict. Especially for modern states and societies where important aspects of civilian life heavily and increasingly depend on a functioning cyber environment, this is a worrying conclusion.

3. Disentangling Military and Civilian Cyber Infrastructure

Of course, a narrower definition of military objectives could help to strike a more adequate balance between military necessity and humanitarian considerations for purposes of the cyber domain, and to better distinguish legitimate targets from protected systems and installations. Politically, however, such an avenue hardly seems viable. Despite the fact that the established definition of military objectives has always been criticised by some authors as being 'so sweeping that it can cover practically anything',[41] if at all, the recent trend has rather been in the direction of further expanding this definition, as is reflected by the controversy over war-sustaining objects on the one hand, or the more recent suggestion of a new subcategory of 'temporary military objectives by nature' on the other.[42]

An alternative way could be to allow only certain forms of attack, namely reversible cyber attacks rather than destructive attacks against such cyber installations that, despite qualifying as military objectives, nevertheless serve a predominantly civilian function. However, it seems utopian to believe that states would or could ever accept a hard and fast obligation to resort only to attacks the effects of which are reversible, notwithstanding the fact that from a strategic point of view it may often make sense to opt for non-destructive attacks and thereby to leave the enemy's cyber infrastructure intact. For the sake of legal coherence and clarity, entirely novel legal concepts – such as a cyber-specific definition of military objectives or a legal obligation to carry out reversible attacks against virtual dual-use targets – would not be conducive in the realm of *jus in bello*. In particular, such an approach would lead to a fragmentation of the humanitarian legal regimes applicable in the cyber domain and other theatres of warfare.[43] Therefore, more plausible solutions may be found on the basis of existing law, namely by way of analogy or extension of the list of objects contained in Article 56 of Additional Protocol I, by reference to

[40] On the Stuxnet attack, see Nicolas Falliere, Liam O Murchu and Eric Chien, 'W32.Stuxnet Dossier' (version 1.4, February 2011), http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

[41] Antonio Cassese, 'Terrorism is also Disrupting Some Crucial Legal Categories of International Law' (2001) European Journal of International Law 993.

[42] Commentary on the HPCR Manual (n 27) 109. For a critique of this approach, see the remarks made by the International Committee of the Red Cross (ICRC) included in a footnote to the Commentary, ibid n 25.

[43] It is, inter alia, for this reason that we reject proposals for a cyber-specific broadening of the range of military targets in the context of cyber attacks; see Jeffrey T G Kelsey, 'Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare' (2008) 106 Michigan Law Review 1427. Moreover, Kelsey's approach is based on the assumed non-lethal nature of cyber attacks, an assumption which in such generality is hardly maintainable.

Article 58(a) and (c) of Additional Protocol I or, perhaps most realistically, by relying on a thorough assessment of proportionality adapted to the technical specificities of cyberspace.

3.1 ARTICLE 56 OF ADDITIONAL PROTOCOL I: EXEMPTING FROM ATTACK IMPORTANT DUAL-USE CYBER INFRASTRUCTURE THAT SERVES IMPORTANT CIVILIAN FUNCTIONS

An alternative to the above mentioned suggestions that, arguably, better responds to the reciprocal interests of states in the maintenance of an overall functionality of cyberspace could be to exclude from the ambit of legitimate military targets, either *per se* or under certain conditions (that is, in cases of minimal use for military purposes), specific cyber infrastructure components, such as the main internet exchange nodes or central servers on which millions of important civilian functions rely.

This approach is neither new nor alien to humanitarian law. Article 56(1) of Additional Protocol I exempts certain objects from attack, even where these objects qualify as military objectives, because of the severe humanitarian consequences an attack on these objects might have.[44] Thus, Article 56(1) lists dual-use objects the destruction of which could release dangerous forces, thereby significantly affecting the civilian population. On the basis of this reasoning, Article 51(1) provides that even other military objectives located in the vicinity of such installations shall not be made the object of attack if such attack may cause the release of dangerous forces and consequential severe losses among the civilian population.

Transposed to the realm of cyberspace, such a *de lege ferenda* approach could be applied to those cyber installations – similar to the objects currently listed in Article 56 of Additional Protocol I – the neutralisation or destruction of which would typically result in significant civilian impact that would outweigh the military benefits. In the realm of cyberspace this approach could help to mitigate repercussions on the civilian population which stem from the fact that central components of the dual-use cyber infrastructure would inevitably always be implicated in military cyber operations, however minimal, and in spite of the fact that they serve primarily civilian functions and may be essential for the overall functionality of civilian cyber traffic. Indeed, in the cyber realm such exemptions would appear to be particularly relevant given that the repercussions on civilian functionality resulting from the neutralisation or destruction of central cyber infrastructure components cannot geographically be confined to the targeted country but may have repercussions for the functionality of cyberspace worldwide.[45]

[44] Dinstein (n 28) 102.

[45] Of course, possible effects on another state's civilian population (ie the civilian population of a state which is not a party to the international armed conflict) belong in the realm of the law of neutrality. Convention (V) respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land (The Hague, 18 October 1907, 205 CTS 229), art 1 stipulates that '[t]he territory of neutral Powers is inviolable', but it remains to be seen how the law of neutrality, especially in as much as it is territory-based, may be applied in the cyber domain and whether the repercussions of a cyber attack directed against State A would be viewed as a violation of the law on neutrality if they also degrade cyber functionality in State B, thereby affecting the civilian population in State B.

Even though there are, in our view, good reasons for excluding certain vital cyber infrastructure components from attacks even where because of their dual nature they qualify as military objectives, analogies to Article 56 or even a *de lege ferenda* extension of this provision to the cyber domain do not appear to be feasible options. First of all, *de lege lata* the exemption provided by Article 56(1) of Additional Protocol I is justified only on the basis of the possibility of 'severe losses among the civilian population'; the civilian impact in the case of attacks against central cyber infrastructure components – although it would most likely be on a very large scale, causing the loss of cyber functionality for thousands of people – would typically not reach a similar level of severity as an attack on a nuclear facility or a dam. Secondly, the destruction of central cyber infrastructure components does not cause dangerous emissions as would the destruction of the objects listed in Article 56. The destruction of central servers may, of course, lead to very widespread, unforeseeable and possibly uncontrollable reverberating effects. However, as the law currently stands, reverberating effects in and of themselves do not satisfy the entry criterion of Article 56 of Additional Protocol I, which requires emissions that are dangerous in and of themselves; their consideration belongs to the realm of the principle of proportionality.

3.2 Segregating Military and Civilian Networks: Article 58 of Additional Protocol I

Of course, a large-scale segregation of military and civilian networks and cyber infrastructure from a humanitarian law point of view would appear to be the most effective measure to enable a clearer distinction between military and civilian objects. Evidently, if civilian networks and civilian cyber infrastructure components are clearly separated from military networks and are thus no longer used for military purposes, the above described dual-use problem is significantly mitigated. Alternatively, at least certain highly sensitive civilian networks and infrastructure pillars, the functionality of which is essential for the civilian population, could be physically removed and disconnected from other networks and the general cyber infrastructure. States may, of course, pursue such approaches for strategic and security reasons. Thus far, however, this has not occurred on any significant scale with respect to civilian systems.[46]

3.2.1 Precautionary Obligations Derived from Article 58(a) of Additional Protocol I

The question at issue is whether international humanitarian law imposes any kind of obligation on states to keep civilian and military networks segregated or to separate such networks and cyber infrastructure components where the coalescence has already occurred. In this context the obligation to take so-called passive precautions (that is, precautions against the effects of attacks) as it is set out in Article 58 of Additional Protocol I[47] – a provision

[46] Jensen (n 10) 1552.
[47] ibid.

https://doi.org/10.1017/S0021223712000179 Published online by Cambridge University Press

which has acquired the status of customary international law and thus applies in both international and non-international armed conflicts – appears to be of central importance.[48] Article 58 in the relevant part provides that '[t]he Parties to the conflict shall, to the maximum extent feasible: a) … endeavour to remove … civilian objects under their control from the vicinity of military objectives'.

However, the obligation laid out in Article 58(a) of Additional Protocol I is subject to a number of limitations. First, all obligations contained in Article 58 are limited by the preceding phrase 'to the maximum extent feasible',[49] which is interpreted to mean that the obligation is limited to those precautions which are practicable or practically possible,[50] taking into account all circumstances ruling at the time, including humanitarian and military considerations.[51] The phrase is reflective of the concerns of various states about the difficulty or impossibility of separation in many instances.[52] The obligation contained in subparagraph (a) is further limited by the use of the word 'endeavour', which arguably qualifies the obligation as being an obligation of conduct rather than an obligation of result.[53] Certainly a large-scale segregation of networks would require a structural remodelling of the entire current technological set-up of cyberspace which, for the time being, is systemically interconnected. It appears doubtful that such a large-scale segregation could be deemed 'practically possible', especially in view of the fact that thus far states have not shown any significant interest – neither economic nor strategic – in disentangling military and civilian cyber infrastructure components in view of the costs and difficulties this would entail.[54]

Secondly, even when leaving aside the question of whether any such structural segregation would be 'feasible' in the sense of Article 58 of Additional Protocol I, the obligation to take passive precautions must not be confused with the question of whether civilian objects may be used for military purposes. International humanitarian law in general and Article 58(a) of Additional Protocol I in particular do not prohibit 'dual use'.[55] Rather, Article 58(a) operates on the

[48] ICRC Study (n 24) rules 22, 23, 24.
[49] This limitation applies to the different obligations laid out in art 58(a)–(c): see Diplomatic Conference leading to the Adoption of the Additional Protocols, Report to Committee III on the Work of the Working Group, 65.
[50] ICRC Study (n 24) Commentary to rule 22.
[51] cf, for instance, the reservation issued by the United Kingdom on the date of its ratification of Additional Protocol I on 28 January 1998, http://www.icrc.org/ihl.nsf/NORM/0A9E03F0F2EE757CC1256402003FB6D2?OpenDocument.
[52] ICRC Study (n 24) Commentary to rule 22.
[53] On this distinction, cf Rüdiger Wolfrum, 'Obligation of Result versus Obligation of Conduct – Some Thoughts about the Implementation of International Obligations' in Mahnoush H Arsanjani and others (eds), *Looking to the Future – Essays on International Law in Honor of W. Michael Reisman* (Martinus Nijhoff 2011) 363.
[54] Jensen (n 10) 1569, who argues that 'the near-complete interconnectedness of government and civilian cyber systems makes segregation under Article 58 (a) and (b) impractical'.
[55] International humanitarian law merely prescribes that civilian objects which are used or intended to be used for military purposes will thereby qualify as legitimate military objectives with the consequence that they could be attacked. A similar regulation is adopted under international humanitarian law where civilians take a direct part in hostilities, thereby losing their protection from attack. Such a direct participation may, of course, amount to a criminal offence under domestic criminal law, but it is not prohibited nor privileged on the level of the *jus in bello*; cf Nils Melzer, *ICRC Interpretive Guidance on the Notion of Direct Participation in Hostilities* (International Committee of the Red Cross 2009) rule X, 83.

assumption that a clear-cut distinction between military targets and protected civilian objects is possible and it is on the basis of this assumption that Article 58 prescribes the segregation of such objects in order to better protect the civilian objects.

The specific problem in cyberspace, however, pertains to the systemic dual-use character of the entire cyber infrastructure and the impossibility to single out – at least with any degree of certainty – networks or infrastructure components that only serve civilian functions. In other words the main problem in cyberspace as it currently exists is not that civilian and military installations are too close together (this being the problem Article 58(a) aims to solve) but that they are one and the same. Structurally this problem and the idea of creating 'digital safe havens'[56] is therefore more akin to the concept of demilitarised zones as envisaged in Article 60 of Additional Protocol I – namely zones that could potentially be used for military operations but where agreement is reached between the parties to an armed conflict not to use such zones for military purposes, rather than the obligation to separate distinguishable military and civilian objects from one another as foreseen by Article 58(a).

In other words, even if states were willing to segregate certain civilian or exclusively military networks from the general cyber infrastructure, they would still need to reach agreement that these civilian networks, given that technically they could still be used for military communications and other military purposes, should be protected and used only for civilian functions. Moreover, given that many military uses of cyberspace relate to concealment, spoofing and manipulation, it is not clear whether exclusively civilian use could ever be ensured or reliably agreed upon. And even if this were possible in times of peace, it is far from clear whether such an agreement could ever be sustained in times of armed conflict because, once the functionality of the military networks is degraded, parties to an armed conflict would most likely turn to still functioning civilian systems as a strategic back-up option. Therefore, as much as we favour the idea of a general and large-scale segregation of military and civilian cyber infrastructure and networks, such a far-reaching remodelling obligation of an entire technology, in our view, cannot be deduced from Article 58(a) of Additional Protocol I.

3.2.2 Precautionary Obligations Derived from Article 58(c) of Additional Protocol I

In addition to Article 58(a), subparagraph (c) of the same provision lays out the general obligation to take *other* necessary precautions to protect the civilian population and civilian objects under the control of the respective party to an armed conflict from the dangers resulting from military operations.[57] The ICRC Commentary mentions preparations for effective fire-fighting as a relevant example for a precaution in the sense of subparagraph (c) in traditional

[56] Adam Segal, 'Cyberspace Governance: The Next Step' (Council on Foreign Relations, Policy Innovation Memorandum No 2, 14 November 2011, 1), http://www.cfr.org/cybersecurity/cyberspace-governance-next-step/p24397.

[57] emphasis added.

https://doi.org/10.1017/S0021223712000179 Published online by Cambridge University Press

contexts.[58] The ICRC Study cites, inter alia, the guarding of civilian property.[59] Like the obligation in Article 58(a) of Additional Protocol I, the obligation to take other precautions in subparagraph (c) is limited by the caveat 'to the maximum extent feasible'.[60] But Article 58(c) goes further in that it requires all kinds of precautions, which means measures taken in advance, that may have protective effects for the civilian population. In light of the overall object and purpose of this provision to better protect the civilian population, transposed to the cyber domain it may thus be argued that states, 'to the maximum extent feasible', will be required to ensure a continuing cyber functionality where such functionality is crucial for the maintenance of critical civilian infrastructure.[61] For example, in a country where the civilian electrical power grid or essential civilian communication systems are heavily reliant on a functioning cyber infrastructure, states – to the maximum extent feasible – will be required to provide back-up modes for the continuing operation of these power grids and communication networks.

4. THE PRINCIPLE OF PROPORTIONALITY

The systemic use of civilian networks and central cyber infrastructure components for military purposes means that the likelihood of adverse repercussions for the civilian population in times of armed conflict is considerably high. Precisely because of this systemic dual use of most cyber components it is rather unlikely, as has been shown above, that states (at least, for the time being) would be willing to agree on rigid solutions such as the general exclusion of certain cyber assets from attack or a legal obligation to disentangle interconnected networks. The general principle of proportionality offers more flexibility in this regard. According to Article 51(5)(b) of Additional Protocol I, which is accepted as having acquired the status of customary international law,[62] 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.[63] There is no controversy about the general applicability of this principle in the cyber domain.[64] Nevertheless, the systemic technological features of cyberspace raise the question as to how the proportionality assessment should be conducted when cyber infrastructure components are the object of an attack.[65] The law is rather straightforward about what may be considered relevant for the purposes of a proportionality assessment: 'Loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof'. In this regard different

[58] ICRC Commentary (n 26) 2258.
[59] ICRC Study (n 24) rule 22.
[60] cf ibid section 3.2.1.
[61] cf Jensen (n 10) 1553.
[62] ICRC Study (n 24) rule 14.
[63] Dinstein (n 28) 128.
[64] Schmitt, 'Wired Warfare' (n 6) 390; Eric Talbot Jensen, 'Unexpected Consequences from Knock-on Effects: A Different Standard for Computer Network Operations?' (2003) 18 American University International Law Review 1145, 1154–61.
[65] For the general difficulties in the application of the humanitarian proportionality principle, see eg Oeter (n 29) 204.

situations should be distinguished. First of all, where cyber infrastructure (still) qualifies as a civilian object and where it is physically destroyed by the side effects of either a conventional military attack or a cyber attack, it must be factored into the proportionality equation as this would clearly amount to damage to a civilian object.

Secondly, however, the more difficult situation arises with respect to dual-use cyber infrastructure that qualifies as a legitimate military objective but simultaneously serves important civilian functions. As has been shown above, as far as attacks on cyber infrastructure components are concerned, this will be a rather typical scenario.[66] Consider the following example: 10 per cent of a central server's capacity is used for military purposes; 90 per cent of its capacity serves civilian functions. The server thus qualifies as a legitimate military objective in line with the questionable but seemingly common understanding that any military use, however minimal, qualifies an entire object as a legitimate military objective. The server is then rendered dysfunctional by way of a cyber attack without any physical destruction of the hardware. Which civilian aspects are relevant for the proportionality assessment in this scenario? Clearly, the server itself as a military objective would not figure within the proportionality equation. However, in view of its dual character and in light of the fact that 90 per cent of its capacity was used for civilian communications and services, there will be widespread loss of functionality for civilian purposes. Nevertheless, in this scenario the assessment of what may be considered as a proportionality-relevant factor is complicated principally for two reasons.

First, it is generally not entirely clear to what degree so-called 'reverberating effects' may be taken into consideration for the purposes of the proportionality calculus in the case of dual-use objects. This, of course, is not a cyber-specific problem. Rather, it is an issue which has been the subject of debate for some time, typically in relation to attacks on electrical power plants.[67] It seems plausible that all 'foreseeable long-term damages'[68] should be considered and that, even if a dual-use object qualifies as a military objective, the adverse civilian side effects that come with its destruction should be considered within the proportionality equation.[69] Indeed, if even minimal military use turns a dual-use object into a legitimate military objective, then at least the adverse civilian impact must be considered as a relevant factor within the proportionality calculus.

Second, in line with the enumeration contained in Article 51(5)(b), it is clear that in any case only the 'loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof' could be considered as relevant collateral damage. Thus, if it is accepted that foreseeable

[66] ibid 7.
[67] Michael N Schmitt, 'The Principle of Discrimination in 21st Century Warfare' (1999) 2 Yale Human Rights and Development Law Journal 143, 168; James W Crawford III, 'The Law of Noncombatant Immunity and the Targeting of National Electrical Power Systems' (1997) 21 Fletcher Forum of World Affairs 101, 106; James A Burger, 'International Humanitarian Law and the Kosovo Crisis: Lessons Learned or to be Learned (2000) 82 International Review of the Red Cross 129, 134.
[68] Oeter (n 29) 181.
[69] Shue and Wippmann (n 13) 565.

reverberating effects are to be included in the proportionality calculus, there still appears to be a limitation to such effects that could be subsumed under the wording of Article 51(5)(b), which is also accepted as customary international law. This means, however, that the mere loss of functionality – in the example provided above a 90 per cent functionality loss of a central server – may generally not enter the proportionality calculus as a relevant factor. Of course, one could arrive at a different conclusion if the phrase 'damage to civilian objects' were seen as broad enough to cover such effects. A systematic argument in this respect may be drawn from a comparison of Article 51(5)(b) and Article 52(2) of Additional Protocol I. Whereas Article 52(2) differentiates between 'destruction' on the one hand and 'neutralisation' on the other, Article 51(5)(b) speaks of 'damage'. It could thus be argued that the word 'damage' as it is used in international humanitarian law comprises both the destruction as well as the neutralisation of an object. Certainly, the word 'damage' does not exclude loss of functionality without physical destruction. In addition, a teleological argument can be drawn from Article 51 in combination with the general rule laid out in Article 48 of Additional Protocol I, the overall purpose of which it is to better protect the civilian population against dangers arising from military operations. It would appear counter-intuitive that only the physical destruction of a civilian object should be taken into consideration, whereas functionality loss – even if it affects the civilian population much more severely – should be irrelevant.

Indeed, a narrow reading of the phrase 'damage to civilian objects' that is limited to physical destruction would lead to the following result. Whereas the destruction of a single civilian car would amount to legally relevant, albeit rather insignificant, 'collateral damage', the disconnection of thousands or millions of households, companies and public services from the internet or other communication services, or the severance of online financial transactions for a country's entire economy and the corresponding economic and societal effects *as such* would not count as relevant elements to be factored into the proportionality calculus. Only when and where these effects foreseeably resulted in the loss of civilian life, injury to civilians or damage to civilian objects could they be considered as factors relevant for the proportionality calculus.[70] Given that it is extremely difficult to determine in advance what the foreseeable physical effects of a large-scale attack against cyber infrastructure components may be – in the interconnected domain of cyberspace such operations may have a number of cascading effects that are hard to predict – the inclusion of direct effects such as the loss of functionality into the list of proportionality-relevant factors would greatly facilitate the application of the proportionality principle, especially in the cyber domain. Evidently, the more cyber-reliant a society is – and in the future this reliance will only increase in a growing number of states – the more detrimental the effects of such functionality loss on the civilian population will be. Much of modern life and indeed vital services in modern societies already rely on a functioning cyber infrastructure. According to the US Department of Defense Strategy for Operating in Cyberspace, 'cyberspace

[70] emphasis added.

https://doi.org/10.1017/S0021223712000179 Published online by Cambridge University Press

will become increasingly woven into the fabric of everyday life across the globe'.[71] Against this background, in line with the overall object and purpose of the humanitarian proportionality principle to mitigate the civilian impact of military operations as far as possible, and in line with the widely accepted expansion of the application of the humanitarian proportionality principle to the cyber domain where almost every object is a dual-use object, we suggest a dynamic interpretation of the wording 'damage to civilian objects', which also considers the loss of functionality of a dual-use object as a relevant factor within the proportionality equation.

5. CONCLUSION

Unlike the natural theatres of war, the artificial domain of cyberspace is made up of physical components. Because of the systemic interconnectedness of networks and systems in cyberspace and the fact that the military currently relies heavily on civilian cyber infrastructure to execute its communications and cyber operations, in times of an armed conflict, on the basis of the law as it currently stands, a wide range of essential components of the cyber infrastructure would legally qualify as legitimate military objectives. This is an alarming conclusion and one that should be acknowledged more widely than it has been to date.

Evidently, if systems which are civilian in nature and serve primarily important civilian interests, such as economic and other societal functions, will nevertheless qualify as legitimate military objectives as a result of their dual use, this will the increase adverse impact on the civilian population. Unfortunately, without further development of the law, there appears to be no completely satisfactory solution to this problem. Of course, theoretically there are a number of solutions that could be drawn from the existing humanitarian legal framework, such as the creation of digital safe havens in cyberspace, or attack exemptions regarding essential cyber installations and infrastructure components that may qualify as legitimate military objectives but serve civilian functions of the highest priority. A segregation of military and civilian networks and cyber infrastructure would arguably best safeguard civilian interests and protection. However, while states are, of course, free to employ such measures, it appears that there is currently no hard and fast legal obligation under the international humanitarian legal framework to adopt any of these solutions.

Thus, while states will be under an obligation to adopt precautions in line with Articles 57 and 58 of Additional Protocol I and their respective customary law pendants, for the time being the principle of proportionality is of crucial importance for the mitigation of adverse impact on the civilian population. In view of an ever increasing reliance on cyber functionality in modern societies, it appears counter-intuitive and outdated to suggest that only the physical destruction of objects should be included in the proportionality calculus. In many instances cyber attacks will not lead to physical destruction but to the loss or degradation of the targeted object's functionality, be it a central server or an electric power plant. Therefore, in line with the widely

[71] US Department of Defense Strategy for Operating in Cyberspace (July 2011, 1), http://www.defense.gov/news/d20110714cyber.pdf.

accepted view that traditional international humanitarian law is applicable also in cyberspace, we suggest a dynamic interpretation of the wording 'damage to civilian objects', an interpretation that also considers the loss of functionality as a relevant factor within the proportionality equation. While similar suggestions have rightly been made with regard to conventional attacks on electricity plants and similar dual-use objects, the humanitarian necessity for an expansion of the range of proportionality relevant factors appears to be of particular urgency in the cyber domain where dual use appears to be the rule rather than the exception.

https://doi.org/10.1017/S0021223712000179 Published online by Cambridge University Press