Volume 94 Number 886 Summer 2012

INTERNATIONAL REVIEW of the Red Cross

Some legal challenges posed by remote attack

William Boothby

Dr William Boothby retired in July 2011 as Deputy Director of Legal Services (Royal Air Force) in the rank of Air Commodore. His doctoral thesis on *Weapons and the Law of Armed Conflict* was published by Oxford University Press (OUP) in 2009 and his second book, *The Law of Targeting*, was published by OUP in August 2012.

Abstract

Attacking from a distance is nothing new, but with the advent of certain new technologies, attacks can be undertaken in which the attacker remains very remote from the scene where force will be employed. This article analyses the legal issues raised by attacks employing, respectively, remotely piloted vehicles, autonomous attack technologies, and cyber capabilities. It considers targeting law principles and rules, including distinction, discrimination, proportionality, and the precautions rules, observes that they all apply to remote attack and proceeds to explore the challenges that arise from implementing the legal requirements. Due note is taken of states' legal obligation to review new weapons, methods and means of warfare, an obligation that reinforces the view that existing law will provide the prism through which these new attack technologies must be evaluated by states. The article then discusses how notions of liability apply in relation to remote attack, and considers whether it is depersonalization rather than remoteness in attack that is the critical legal issue.

Keywords: remote attack, remotely piloted vehicles, unmanned aerial vehicles (UAVs), cyber attack, autonomous attack, legal review of new weapons, means or method of warfare, liability.

In a report dated 29 November 2011, *The Guardian* newspaper asked '[w]hy did NATO forces kill two dozen Pakistani soldiers at a border post in the Mohmand

doi:10.1017/S1816383112000719

region, some 300 yards across the frontier from Afghanistan early on Saturday morning?'[1] Having reflected upon differing explanations for the event, the report asserted '[t]here is a very simple explanation of what happened, the US military makes deadly mistakes all the time, and for all its technological wizardry and tremendous firepower, it has very little intelligence on the ground'. Reportedly, in 2010 'a U.S. military investigation . . . harshly criticized a Nevada-based Air Force drone crew and American ground commanders in Afghanistan for misidentifying civilians as insurgents during a U.S. Army Special Forces operation in Oruzgan province in February, resulting in the deaths of as many as 23 civilians'.[2]

From one kind of 'military operations from a distance', or remote attack as we shall call the phenomenon, let us move to another, namely cyber operations. Military use of cyber operations[3] occurred on 27 and 28 April 2007 when an apparently coordinated sequence of denial-of-service operations affected websites in Estonia during a dispute between that country and Russia. Ping requests were followed by malformed Web queries to governmental and media websites. From 30 April until 18 May 2007, distributed operations aimed at producing a denial of service from targeted websites (distributed denial of service or DDoS) followed. Careful timing of cyber operations maximized their effectiveness, and the affected sites became temporarily inaccessible. It appeared that botnets were being employed and a precise impact was the evident result.[4] Some Estonian websites were defaced by so-called patriotic hackers, but it was never formally determined which state, if any, was responsible.[5] Then, in 2008, cyber operations were undertaken against Georgia during its armed conflict with Russia.

The 2010 Stuxnet operation against Iran was, perhaps, one of the more militarily significant cyber operations. Stuxnet is an integrated set of components that were used to undertake computer network attacks. Using, in part, a worm as its delivery mechanism, Stuxnet inserts itself onto disconnected networks, for example through the use of thumb drives or CD-ROMs. It searches for a specified manufacturer's model of computer control facility – in the case of the Iranian attack

1 P. Chatterjee, 'Should we allow NATO free rein to attack and kill people?', in *The Guardian,* 29 November 2011, available at: http://www.guardian.co.uk/commentisfree/2011/nov/29/nato-free-range-to-kill (this and all subsequent links last visited April 2012).

2 For reference to the earlier cited incident, see David Zucchino, 'US Report faults Air Force drone crew, ground commanders in Afghan civilian deaths', in *Los Angeles Times*, 29 May 2010, available at: http://articles.latimes.com/2010/may/29/world/la-fg-afghan-drone-20100531.

3 Cyber operations are taken for the purposes of this article to consist of the use of a computer to interact with another computer for purposes linked to a military operation. Cyber attack is therefore, for similar purposes, the use of a computer to target another computer and thus to cause violent effects, consisting of damage or destruction to property or death or injury to persons. See Michael N. Schmitt, 'Cyber operations and the *jus in bello*: key issues', in *International Law Studies*, Vol. 87, 2011, pp. 93–94.

4 Eneken Tikk, Kadri Kaska and Liis Vihul, *International Cyber Incidents: Legal Considerations*, CCD COE Publications, Talllinn, 2010, pp. 18–25. Note also that a DDoS operation on 26–28 April 2008, which targeted the website of Radio Free Europe/Radio Liberty's Belarus service, is reported and discussed at E. Tikk, *ibid*., pp. 39–48, as is a cyber operation that targeted Lithuania on 17 June 2008, E. Tikk, *ibid*., pp. 51-64.

5 William A. Owens, Kenneth W. Dam and Herbert S. Lin, *Technology, Policy, Law and Ethics Regarding US Acquisition and Use of Cyberattack Capabilities*, National Research Council of the National Academies, The National Academies Press, Washington D.C., 2009, pp. 173–176.

https://doi.org/10.1017/S1816383112000719 Published online by Cambridge University Press

INTERNATIONAL REVIEW of the Red Cross

a control system manufactured by Siemens – finds and places itself on a relevant node and undertakes pre-planned activity. During the July 2010 operation, malware reportedly attacked centrifuges evidently associated with the Iranian nuclear programme and, it appears, caused damage.[6] While the defacement of websites as exemplified in the Estonian operations would not seem to amount to an attack in the *in bello* sense,[7] it is likely that the Stuxnet attack would be regarded at law as such an attack because of the damage reportedly caused to the centrifuges.

The use, during armed conflicts, of these cyber techniques to prosecute attacks, that is to cause death, injury, damage or destruction, or the employment of remotely piloted[8] or, in the future, autonomous unmanned platforms to undertake attacks constitutes what, for the purposes of this article, we shall describe as 'remote attack'. Such attacks are remote in the sense that the operator of the remotely piloted vehicle or the initiator of the autonomous mission or of the cyber attack is liable to be located at a considerable distance from the scene of the injury or destruction wrought by the attack. The purpose of the present article is to consider whether the remote conduct of attacks using such techniques during armed conflicts raises legal concerns. The author's starting point is that cyber attacks during armed conflict, namely military operations in which cyber means are employed to inflict death, injury, damage or destruction on an adverse party to the conflict, are regulated by the law of armed conflict and thus, for states party to the Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (API),[9] are subject to the rules in Articles 48 to 67 of that treaty.[10] For states that are not party to API, the customary principles and rules – most notably the customary principle of distinction and the customary rules of discrimination, of proportionality, and of precautions in attack – will

6 It is understood that these reports of damage have not been confirmed by Iran. See, however, Jonathan Fildes, 'Stuxnet worm "targeted high value Iranian assets"', in *BBC News*, 23 September 2010, available at: http://www.bbc.co.uk/news/technology-11388018; and William J. Broad, John Markoff and David E. Sanger, 'Israeli test on worm called crucial in Iran nuclear delay', in *New York Times*, 15 January 2011, available at: http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all.

7 See Article 49(1) of API, which defines attacks in terms of the use of violence, whether in offence or defence.

8 As to the controversies raised by the use of unmanned platforms to conduct attacks during current operations, see for example Karen DeYoung, 'U.S. officials cite gains against Al-Qaeda in Pakistan', in *Washington Post*, 1 June 2009, available at: http://www.washingtonpost.com/wp-dyn/content/article/2009/05/31/AR2009053102172.html; the associated analysis by Kenneth Anderson in 'The continuing predator drone campaign in Pakistan', in *Opinio Juris Blog*, 1 June 2009, available at: http://opiniojuris.org/2009/06/01/the-continuing-predator-drone-campaign-in-pakistan/; and Karen DeYoung, 'CIA idles drone flights from base in Pakistan', in *Washington Post*, 1 July 2011, available at: http://www.washingtonpost.com/world/national-security/cia-idles-drone-flights-from-base-in-pakistan/2011/07/01/AGpOiKuH_story.html. As to US appreciation of the strategic importance of attacks on Al Qaeda often carried out using unmanned platforms, see Eric Schmitt and Mark Mazzetti, 'Obama adviser outlines plans to defeat Al Qaeda', *New York Times*, 29 June 2011, available at: http://www.nytimes.com/2011/06/30/world/30terror.html.

9 Adopted in Geneva, 8 June 1977.

10 For a discussion of this issue, see Michael N. Schmitt, 'Cyber operations and the *jus in bello*: key issues', in *US Naval War College Blue Book*, 'International Law and the Changing Character of War', Vol. 87, 2011, p. 89.

https://doi.org/10.1017/S1816383112000719 Published online by Cambridge University Press

apply.[11] Similarly, it seems to be generally accepted that the same body of law regulates attacks using unmanned platforms, that is aircraft, ground vehicles, ships or other marine craft that do not carry crew personnel and that are either controlled by an operator who is located remotely from the relevant platform or that employ autonomous guidance and attack technology.[12] We will discuss these issues primarily by reference to the air domain and will call such operator-controlled vehicles 'remotely piloted vehicles', while references to autonomy will be applied to platforms that make attack decisions without the supervision of a human being. In relation to both such methods of attack, the question to be discussed is therefore whether the absence of the person who is undertaking the attack from the location of its operative effect raises legal concerns.

We shall start by considering attacks using remotely piloted platforms. We will then briefly outline the issues in relation to precautions in attack posed by the use of autonomous attack technologies. In the third section of the article we will summarize how the targeting rules in API can be applied to cyber attacks. Then, in the fourth section, we will analyse where the remoteness challenge sits. In the fifth section we will discuss where liability may rest for these differing classes of attack. In the final substantive section we will ask whether these new technologies represent a qualitative change in the conduct of warfare or a further development in a well-established evolutionary process, essentially posing the question whether what we are discussing is really anything substantively new. We will then seek to draw conclusions.

Remotely piloted vehicles and the law

The remoteness of the controller from the attack does not, per se, exclude the application of targeting law to such activities. The legal principle of

11 In practice, many of the rules in API, Articles 48 to 67, are customary in nature and thus bind all states; see Jean-Marie Henckaerts and Louise Doswald-Beck, *Customary International Humanitarian* Law, *Vol. 1: Rules*, Cambridge University Press, 2005 (hereafter 'ICRC Study'). While in the view of the present author the rules in Articles 35(3), 55 and 56 of API have not achieved customary status, note for example the principle of distinction as reflected in the ICRC Study, rule 1 at page 3: 'The parties to the conflict must at all times distinguish between civilians and combatants. Attacks may only be directed against combatants. Attacks must not be directed against civilians'. Note also the International Court of Justice (ICJ) finding that the principle of distinction is 'an intransgressible principl[e] of international customary law', International Court of Justice, *Advisory Opinion on the Threat or Use of Nuclear Weapons*, ICJ Reports, 8 July 1996, p. 257, para. 79. The ICRC Study reflects the principle of discrimination in its rule 11 at page 37, rule 12 at page 40, rule 13 at page 43, and rule 14 at page 46. These rules respectively prohibit indiscriminate attacks, spell out what such attacks comprise, and then reflect Article 51(5)(a) and (b) of API which, it will be recalled, are described in the treaty as examples of indiscriminate attacks. Customary law also recognizes a rule that requires attackers to take certain precautions in attacks. These customary precautionary rules are reflected in the ICRC Study at rules 18 to 21 on pages 58 to 65. For a discussion of the customary law of targeting, see William H. Boothby, *The Law of Targeting*, Oxford University Press, Oxford, 2012, Chapter 5.

12 See, for example, the discussion in 'Targeting operations with drone technology: humanitarian law implications', in *Background Note for the American Society of International Law Annual Meeting*, Human Rights Institute, Columbia Law School, 25 March 2011.

https://doi.org/10.1017/S1816383112000719 Published online by Cambridge University Press

distinction,[13] the prohibition of indiscriminate attacks,[14] the precautions rules, and the more detailed provisions requiring the protection of specific persons and objects[15] will all apply to such operations. The controller of a Predator or Reaper Unmanned Aerial Vehicle (UAV), although located some thousands of miles from the scene of the attack, bases his attack decisions on the information derived from sensors and other sources and is as constrained by the targeting rules, including the rules as to precautions in attack, as any other military operator in the battle space, including a pilot of a manned aircraft.

Accordingly, the UAV operator must take constant care to spare civilians and civilian objects when undertaking military operations in general;[16] he must do everything practicable or practically possible[17] to 'verify that the objectives to be attacked are neither civilians nor civilian objects and are not subject to special protection but are military objectives . . . and that it is not prohibited . . . to attack them'; he must take all practicable or practically possible precautions in the choice of means and methods of attack with a view to avoiding, and in any event to minimizing, incidental loss of civilian life, injury to civilians and damage to civilian objects;[18] he must 'refrain from deciding to launch any attack which may be expected' to cause disproportionate incidental civilian injury and/or damage;[19] he must cancel or suspend the attack if it becomes clear that its objective is not a military objective, that its objective is subject to special protection or that the attack may be expected to cause disproportionate incidental civilian injury or damage;[20] he must ensure that an effective advance warning is given if civilians may be affected by the attack unless circumstances do not permit;[21] and he must ensure that 'when a choice is possible between several military objectives for obtaining a similar military advantage, the objective that is selected is the objective 'the attack on which may be

13 Article 48 of API requires that 'in order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives'. The notion of 'military objective' is defined, so far as objects are concerned, in Article 52(2) of API.

14 By virtue of Article 51(4) of API, attacks are indiscriminate and therefore prohibited if they are not directed at a specific military objective, if they employ a method or means of combat that cannot be directed at a specific military objective, or the effects of which cannot be limited as required by international law, and in any such case are of a nature to strike the military objective and civilians or civilian objects without distinction. An attack that may be expected to cause excessive incidental injury to civilians and/or damage to civilian objects is stated at Article 51(5) to be an example of an indiscriminate attack.

15 For example, the prohibitions on making the civilian population, individual civilians, or civilian objects the object of attack in Articles 51(2) and 52(1) of API.

16 Article 57(1) of API.

17 The language used in Article 57(2)(a)(i) is 'everything feasible', which the UK interprets as everything 'practicable or practically possible taking into account all circumstances ruling at the time including humanitarian and military considerations'; UK statement (b) made on ratification of API on 28 January 1998. Consider also Eritrea/Ethiopia Claims Commission, *Partial Award, Central Front, Ethiopia's Claim 2*, 28 April 2004, para. 110, available at: http://www.pca-cpa.org/showpage.asp?pag_id=1151.

18 Article 57(2)(a)(ii) of API.

19 Article 57(2)(a)(iii) of API.

20 Article 57(2)(b) of API.

21 Article 57(2)(c) of API.

https://doi.org/10.1017/S1816383112000719 Published online by Cambridge University Press

expected to cause the least danger to civilian lives and to civilian objects'.[22] These precautionary rules bind parties to API as a matter of treaty law and, as we noted above, are largely customary and thus bind all states. It follows from this analysis that the precautionary duties of a controller of an armed UAV are just as exacting as those imposed on the pilot of a manned aircraft. The law does not reduce these duties because of the absence of a person from the cockpit.[23]

Autonomous attack and the law

The word 'autonomy' is taken for the purposes of the present discussion to refer to autonomous attack decision-making undertaken by, for example, algorithm-based technology on board an unmanned platform such as an aerial vehicle.[24] The technology may, for example, be programmed to detect points of recognition of particular military objects, such as a tank, artillery piece or armoured personnel carrier. If the technology adequately distinguishes between such military objects and civilian objects, it would seem that the requirement in Article 57(2)(a)(i) of API[25] may be complied with, provided it can properly be said that 'everything feasible' is being done to accomplish the required distinction. In the light of the United Kingdom (UK) interpretative statement cited above,[26] military considerations may be taken into account in order to determine that which is practically possible and thus required as a feasible precaution. An argument that the absence of a human being from the autonomous aspect of the decision-making process renders the performance of these precautionary duties impractical and that they are therefore to be regarded as militarily non-feasible would, in the author's view, be unsatisfactory, not least because alternative methods of undertaking such attacks would permit of the taking of such precautions. The better view must therefore be that the full set of precautionary measures set out in Article 57 of API and summarized in the previous section of this article must be complied with in relation to autonomous attacks.

While compliance with Article 57(2)(a)(i) of API may be achievable as discussed in the previous paragraph,[27] things get somewhat more difficult when we

22 Article 57(3) of API.

23 The interesting question is whether the absence of a person from the cockpit renders compliance with the rules easier or more difficult. Providing an answer would involve considering whether direct, as opposed to sensor-based observation of the intended target by the person deciding on the particular attack would have been feasible in the relevant circumstances had a manned platform been used; whether such direct observation in the prevailing circumstances would have made any difference to the quality of attack decision-making; whether enemy action may have diverted the pilot's attention from the targeting task; whether other distractions would have been present; and relevant and numerous other issues.

24 The word 'autonomy' is sometimes used to refer to aspects of the navigational system of the platform. In the present article, it specifically refers to the method of attack, and particularly to the method whereby the weapon's target is selected.

25 This requirement is customary in nature; see rule 18 of the ICRC Study and the discussion at W. Boothby, above note 11, p. 73.

26 See above note 17.

27 See Bill Boothby, 'The law relating to unmanned aerial vehicles, unmanned combat aerial vehicles and intelligence gathering from the air', in *Humanitäres Völkerrecht – Informationsschriften*, Vol. 24, issue 2, 2011, p. 81.

https://doi.org/10.1017/S1816383112000719 Published online by Cambridge University Press

consider the evaluative rules of precaution. These further precautionary duties, listed in the previous section and which do not require repetition here, generate the challenging question of whether technology is capable of mechanizing essentially evaluative judgements. These include the assessment of whether the chosen means and method for undertaking the planned attack will in fact minimize injury to civilians and damage to civilian objects and whether the injury to civilians and the damage to civilian objects that may be expected to result from the attack of a given class of military objective on a specified occasion will be excessive in relation to the anticipated military advantage. The statement by the UK and other states on ratification of API, to the effect that military advantage is intended to refer to that accruing from the attack considered as a whole,[28] suggests that the proportionality assessment should be applied to something more that an individual engagement of a single object.[29]

Nevertheless, a means or method of warfare[30] is likely to prove legally unacceptable if it precludes the taking of these legally required evaluative precautions. Autonomous attack methods will not, however, necessarily preclude the taking of these precautions. Thus, planners and operational decision-makers contemplating the mounting of an autonomous mission are likely to be in a position to review relevant pattern-of-life data relating to the planned area of search. They will review that data in order to assess, before the commencement of the autonomous mission, the civilian death, injury, and damage that may be expected as a result of an attack of the planned class of military objective in that area during the planned period of search using the weapons loaded onto the platform. The military advantage to be anticipated from the successful attack of an object that the algorithm technology is programmed to recognize will be known at the planning stage, so, depending on the pattern of life in the relevant area, it may be possible to comply with the evaluative precautionary rules at the mission planning stage thus rendering the use of autonomous attack technology potentially lawful. This is most likely to be the case if the planned area of search is remote from civilians and civilian objects; areas of desert, remote steppe lands, and remote maritime areas would seem to be examples. It may also be the case if, for whatever reason, pattern-of-life data clearly show that civilians will remain absent from a less remote area at the time of the planned search.

If, by contrast, judgements as to the minimization of civilian death, injury, and damage and as to the proportionality of attacks cannot be made at the sortie planning stage, for example because of the congested urban nature of the area of

28 UK statement (i) made on ratification of API on 28 January 1998.

29 The statement was made by reference to Articles 51 and 57. Viewing individual hostile acts in isolation 'would ignore the problems resulting from modern strategies of warfare, which are invariably based on an integrated series of separate actions forming one ultimate compound operation . . . The aggregate military operation of the belligerent may not be divided up into too many individual actions, otherwise the operative purpose for which the overall operation was designed slips out of sight'. Stefan Oeter, 'Methods and means of combat', in D. Fleck (ed.), *The Handbook of International Humanitarian Law*, 2nd edn, 2009, p. 186.

30 The particular platform will form part of the weapon system associated with the relevant missile, etc. It will be a part of that means of warfare.

https://doi.org/10.1017/S1816383112000719 Published online by Cambridge University Press

search or because for whatever reason civilian death, injury, and damage cannot be predicted with acceptable assurance in advance of the mission, it follows that the evaluative precautions cannot be undertaken with the consequence that a decision to undertake an autonomous mission in such circumstances would breach Article 57.

The focus in this discussion is on autonomous attacks targeting inherently military objects with characteristics that facilitate mechanical recognition. So far as is known, technology is not currently available to support the autonomous distinguishing of military personnel from civilians. Only when autonomous attack technology can make those distinctions to an acceptable degree of reliability, and only when, having so distinguished, the technology enables the evaluative decisions referred to above to be made in the context of attacks that target persons will there be any basis for a discussion of autonomous attack of individuals. The author is not aware of any such system yet having been fielded, and therefore concludes that autonomous attack of personnel can, for the time being at least, be excluded on the ground that the rules as to precautions in attack cannot be complied with.[31]

Cyber attacks and the law

The computer age has brought into existence another environment in which hostilities can be conducted.[32] The dependence of modern societies and of their armed forces on computer systems renders such systems prime objects of attack, or a choice medium through which to target some linked object or person.[33] Events in Estonia in 2007,[34] in Georgia in 2008[35] and in Iran in

31 See, however, Ronald C. Arkin, *Governing Lethal Behavior in Autonomous Robots*, CRC Press Taylor & Francis Group, Boca Raton, F.A., 2009, for a discussion of technical approaches to robotic decision-making designed to overcome the issues discussed in the present section. For a statement of the technological requirements before autonomous attack is likely to become legally acceptable, see Tony Gillespie and Robin West, 'Requirements for autonomous unmanned air systems set by legal issues', in *The International C2 Journal*, Vol. 4, No. 2, 2010, pp. 1–32, available at: http://www.dodccrp.org/files/IC2J_v4n2_02_Gillespie.pdf. For a suggested ethical duty to use UAVs, see Bradley J. Strawser, 'Moral predators: the duty to employ uninhabited aerial vehicles', in *Journal of Military Ethics*, Vol. 9, No. 4, 2010, pp. 342–344. Ronald C. Arkin, 'The case for ethical autonomy in unmanned systems', in *Journal of Military Ethics*, Vol. 9, No. 4, 2010, pp. 332, analyses why humans breach the legal and moral prohibition of attacking civilians and argues that robotic attack techniques will tend to obviate such unacceptable behaviour.

32 The word 'environment' is used because views differ as to whether cyberspace can properly be described as a 'domain'; see Michael V. Hayden, 'The future of things "cyber"', in *Strategic Studies Quarterly*, Vol. 5, No. 1, Spring 2011, pp. 3–4; and John A. Shaud, 'An Air Force strategic vision for 2020–2030', in *Strategic Studies Quarterly*, Vol. 5, No. 1, Spring 2011, pp. 8–17.

33 Note, for example, the May 2009 cyber operation that shut down the US FBI computer network; Bill Gertz, 'Inside the ring', in *The Washington Times*, 18 June 2009, available at: http://www.washingtontimes.com/news/2009/jun/18/inside-the-ring-95264632/?page=all; for an indication of the scale and extent of cyber espionage, see Sean Rayment, 'How safe are Britain's cyber borders?', in *The Sunday Telegraph*, 26 June 2011, available at: http://www.telegraph.co.uk/news/uknews/defence/8598952/How-safe-are-Britains-cyber-borders.html.

34 See E. Tikk, *et al.*, above note 4, pp. 18–25; and W. A. Owens, *et al.*, above note 5, pp. 173–176.

35 J. Markoff, 'Georgia takes a beating in the cyberwar with Russia', in *New York Times*, Bits Blog, 11 August 2008, available at: http://bits.blogs.nytimes.com/2008/08/11/georgia-takes-a-beating-in-the-cyberwar-

https://doi.org/10.1017/S1816383112000719 Published online by Cambridge University Press

2010[36] indicate that the offensive use of cyber operations will be an increasingly important aspect of warfare in coming decades. Cyber operations can be taken to be military operations in which one computer is used either to target another or to use that other computer as the conduit through which injury or damage is caused to an opposing party to the conflict. The use of any instrument, including a computer, to cause death, injury, damage or destruction to another party to an armed conflict will cause that instrument, or computer, to become a weapon or means of warfare.[37] The damage or injury may be caused to the users of the targeted computer system or the targeted system itself may be damaged; in either case causing the cyber operation to be regarded as a cyber attack. The critical issue for the purposes of the present article is, however, that the operation may be initiated a considerable distance in both space and time from the place and time, where and when, the damaging consequences are intended to occur. This notion of remoteness of the operator from the consequences of his or her activity is compounded by the difficulty that is likely to be encountered in determining, and then being able to demonstrate, first, who undertook the cyber operation in question, second, on behalf of which state or organization, if any, the operation was undertaken, and, third, its purpose.

A relevant legal issue arises from the difficulty that the planner and decision-maker are likely to have in evaluating in advance the expected results of a planned cyber attack. In order to make any sensible assessment of the legitimacy of the planned attack they will need to know enough about the cyber linkages between the sending computer and the targeted computer to be sufficiently assured that the attack will in fact engage the intended target. Secondly, they will also need to know enough about the characteristics of the particular cyber capability that is being used to undertake the attack to be assured that it will engage the target in the intended way. Thirdly, they will need to know enough about the targeted computer system, its dependencies, and associated networks to be able to assess the proportionality of the planned attack. Finally, if the cyber capability to be used in the attack is liable to affect other networks as it travels to the targeted system, the expected effects on those other networks will need to be assessed as, to the extent that those networks do not themselves consist of military objectives, damage to them, and consequential damage or injury to their users will have to be factored into the proportionality assessment that is made in advance of the decision to mount the cyber attack.

Mapping the targeted system, its dependencies, and the intervening linkages in this way is likely to be a challenging task. Undertaking that mapping in a covert way is likely to be even more difficult. To maintain that operational security by failing to undertake any assessment of the proportionality of the planned attack

with-russia/; European Union Independent International Fact Finding Mission on the Conflict in Georgia, Report (2009); and see also E. Tikk, *et al.*, above note 4, pp. 67–79.

36 J. Fildes, 'Stuxnet worm attacked high value Iranian assets', in *BBC News*, 23 September 2010, available at: http://www.bbc.co.uk/news/technology-11388018; and W. J. Broad, *et al.*, above note 6.

37 For the meaning of weapon see Justin McClelland, 'The review of weapons in accordance with Article 36 of Additional Protocol 1', in *International Review of the Red Cross*, Vol. 85, No. 850, June 2003, p. 397. For the meaning of 'means of warfare', see William H. Boothby, *Weapons and the Law of Armed Conflict*, Oxford University Press, Oxford, 2009, p. 4.

https://doi.org/10.1017/S1816383112000719 Published online by Cambridge University Press

is likely to breach Article 57 for the same reasons as were noted in the previous section.

Where the remoteness challenge sits

What emerges from the analysis, however, is that the distance in time and space does not of itself render the attack unlawful. At the root of the problem is the effect that this remoteness has on the ability of planners and decision-makers to undertake required precautions and to obtain information to support a sensible evaluation of the lawfulness of the planned attack. To put the matter simply, it is only when the technological advances that enable remote attack, be it cyber, autonomous or remotely piloted, are matched by the technological capability to inform the standard precautions the law requires in relation to all attacks that the use of such remote attack capabilities becomes lawful. This has been broadly achieved and demonstrated in respect of remotely piloted missions. Clearly, as the opening paragraphs of this article demonstrate, there are occasions when errors are made, but the making of errors does not call into question the lawfulness of the method of warfare as such. Rather, it is whether the method is capable of being employed in accordance with established legal requirements that is the critical issue under weapons law.[38]

As the previous section made clear, in certain narrowly defined generic circumstances autonomous attacks are also capable of being conducted in accordance with the requirements of the law of armed conflict. In the cyber domain, however, much will depend on the particular cyber tool that it is planned to use, on the characteristics of that tool, on whether the damaging effect of the cyber tool can be reasonably limited to the intended target of attack, and on whether enough is known about the target computer system to enable proper precautionary judgements of the sort discussed above to be made.

API requires that 'in the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by [API] or by any other rule of international law applicable to the High Contracting Party'.[39] Having concluded that cyber capabilities that are to be used to cause death, injury, damage or destruction to an opposing party to a conflict are means of warfare for the purposes of Article 36, it is clear that a legal review of such capabilities will be required and that the matters discussed in the previous paragraph will need to be considered when deciding whether the capability is indiscriminate by nature.[40]

38 For a discussion of the application of the law of armed conflict to cyber operations, see Charles J. Dunlap, 'Perspectives for cyber strategists on law for cyberwar', in *Strategic Studies Quarterly*, Spring 2011, pp. 81–99.

39 Article 36 of API.

40 W. H. Boothby, above note 37, pp. 69–85 and 345–347.

https://doi.org/10.1017/S1816383112000719 Published online by Cambridge University Press

INTERNATIONAL REVIEW of the Red Cross

Liability considerations

Liability for error in remote attack

Legal discussion of remote attack technologies often centres on the question of responsibility. Who is responsible when something goes wrong? In the case of cyber attacks it may be very difficult to determine who precisely undertook the attack and with what particular purpose. The computer from which the attack was initiated may in some cases be identifiable, but the name of the person who created the cyber weapon, the name of the potentially different person who sent the cyber weapon on its way and the state, group, or other entity for which these persons were acting may never be known or capable of public disclosure. These difficulties may therefore make it impossible in practice to fix liability in the case of particular cyber events.

Responsibility, and the related notion of liability, can arise in differing contexts, including at the political/diplomatic level, in the media, at international law, and in domestic law. It may take the form of individual, including command, or state responsibility.

Media coverage of an incident may inform, or drive, perceived political responsibility for the event, as indeed political appreciations may influence media coverage. Early media reports, which may be based in whole or in part on flawed information, speculation, and assumption, and the responses thereto, may fix in the public mind a perception of responsibility that may be hard later to dispel if more reliable data come to light. Early disclosure by governments of factual data, including imagery, may be critical here. This implies, in policy terms, a need to have relevant information readily available in disclosable form if states are to engage successfully in the modern information and media campaigns. Responsibility tends to be attributed by the media to states, but if evidence of individual wrongdoing emerges within the period of active press interest the relevant persons may also attract critical media comment.

When it comes to attributing legal responsibility, judgements after the event must be based on the information, from all sources, that was reasonably available to the decision-maker at the relevant time.[41] In the case of an attack using a remotely piloted vehicle, the decision by the platform controller to undertake that attack will have been informed by the data fed to him when he was considering and making that decision. The vital issue will be whether that controller's decision to attack was reasonable in the circumstances as they were presented to him. Relevant questions may include whether there were any additional practicable precautions that were not taken and that, if taken, would have verified the status of the target as a military objective, whether the attack could be expected to be proportionate and whether it was being undertaken so as to minimize civilian injury and damage.[42]

41 See statement (c) made by the UK on ratification of API on 28 January 1998.

42 Note in this regard the observation in the UK Manual that the level at which legal responsibility to take precautions in attack rests is not specified in API, that whether a person has this responsibility will depend on whether he has any discretion as to the way in which the attack is carried out, and that the responsibility will therefore range from Commanders in Chief and their planning staffs to individual

https://doi.org/10.1017/S1816383112000719 Published online by Cambridge University Press

It follows that if the relevant equipment was operating properly,[43] the operator of the platform is liable for his actions in relation to that platform. However, if for example the data feeds to the controller were adversely affected by a system fault, and if that fault can properly be said to have caused the erroneous decision to attack, then the system failure is likely to exonerate the controller from responsibility for the attack.

Similarly, if the opposing party to the conflict, whether through ruses, perfidy, voluntary or involuntary human-shielding or otherwise, materially impedes the platform operator's task, that will also be a factor to take into account when determining responsibility for the resulting events. It would not seem to be reasonable to lay blame at the door of the operator for errors attributable to the supporting systems, enemy action or other causes beyond his control. Whether the erroneous attack truly was beyond the operator's control will, however, be a question of fact to be assessed when all relevant information is available. It would seem that the factors to consider when determining potential liability of the controller of a remote platform are essentially similar to those that apply, for example, in the case of a pilot undertaking a similar mission.

There is no war crime of failing to take precautions in attack. Relevant war crimes under the Rome Statute, for example, would include directing attacks at civilians,[44] directing attacks at civilian objects[45] and prosecuting disproportionate attacks.[46] The intent that is an ingredient of these offences is not of course to be equated with a failure to take the required precautions, although in particular factual circumstances such a failure may be an element in such an intentional attack. Command responsibility would also be determined on a similar basis to that applying in relation to more conventional military operations, for example bombardment from piloted aircraft. A military commander is criminally responsible under the Rome Statute for crimes committed by forces under his or her effective command and control as a result of his or her failure to exercise control properly over such forces. The provision requires that either the military commander knew, or in the circumstances at the time should have known, that the forces were committing or about to commit such crimes and that he or she failed to take 'all necessary and reasonable measures within his or her power to repress or

soldiers opening fire on their own initiative; those carrying out orders for an attack must cancel or suspend it if the object to be attacked is such that the proportionality rule will be breached. *UK Joint Service Manual of the Law of Armed Conflict*, UK Ministry of Defence, 2004, para. 5.32.9.

43 This is an important caveat – opposing forces may be deliberately corrupting the image, impeding the operation of critical sensors, or using spoofs or other ruses to distort the picture.

44 Article 8(2)(b)(i) of the Rome Statute of the International Criminal Court, 1998 (hereinafter 'Rome Statute') provides for the crime of 'intentionally directing attacks against the civilian population as such or against individual civilians not taking direct part in hostilities'.

45 Article 8(2)(b)(ii) of the Rome Statute provides for the offence of 'intentionally directing attacks against civilian objects, that is, objects that are not military objectives'.

46 Article 8(2)(b)(iv) of the Rome Statute provides for the offence of 'intentionally launching an attack in the knowledge that such attack will cause incidental loss of life or injury to civilians or damage to civilian objects or wide-spread, long-term and severe damage to the natural environment which would be clearly excessive in relation to the concrete and direct overall military advantage anticipated'.

https://doi.org/10.1017/S1816383112000719 Published online by Cambridge University Press

INTERNATIONAL REVIEW of the Red Cross

prevent their commission'.[47] While the failure being discussed in the present article, namely the failure to take adequate precautions, does not amount to a war crime under the Rome Statute, any argument that commanders are also responsible for the failure is likely to be assessed according to similar criteria. Ultimately, the issue will be whether the commander knew, or ought to have known, that the method of attack being adopted precluded taking required precautions. It seems most likely that commanders would be aware of this.

Liability for lawful attacks

Generally speaking there is no liability at law for action by the armed forces of one party to an international armed conflict that lawfully causes death, injury, damage or destruction to an opposing party to the conflict.[48] To be lawful, such action must comply with the law of international armed conflict. Thus there is no liability for the damage lawfully done to military objectives, for the death or injury lawfully caused to members of the opposing armed forces, for expected death, injury or damage to civilians or civilian objects which is not excessive in relation to the anticipated concrete and direct military advantage, or for the death or injury of civilians or damage to civilian objects caused by mistaken or erroneous attacks caused, for example, by the malfunction of military equipment.

The liability to compensate provided in Article 3 of Hague Convention IV, 1907[49] is repeated in similar terms in Article 91 of API.[50] Applying Article 91, it would therefore seem that if, as a result of the failure to take all feasible precautions in relation to a remote attack operation, the attack causes excessive death or injury to civilians or excessive damage or destruction to civilian objects in relation to the concrete and direct military advantage anticipated there is likely to be a legal liability to compensate the affected civilians or civilian institutions if the case so demands. The API Commentary suggests that a simple violation of the law of armed conflict is not sufficient, that there must have been loss or damage and that compensation will only be appropriate if restitution in kind or the restoration of the pre-existing position is not possible.[51] This would suggest that, in order to establish liability, the claimants would need to prove that legally required precautions were not

47 Article 87 of API, and Article 28 of the Rome Statute.

48 The lawfulness of the action precludes liability of the state that undertook the attack in question; Hague Convention IV, Article 3, requires that there has been a violation. As to liability of individual combatants, Article 43(2) of API provides that members of the armed forces are combatants, that is they have the right to participate directly in hostilities.

49 The Article provides: 'A belligerent party which violates the provisions of the said Regulations shall, if the case so demands, be liable to pay compensation. It shall be responsible for all acts committed by persons forming part of its armed forces'.

50 This Article is in similar terms to Article 3 of Hague Convention IV, 1907, save that Article 91 refers to breaches of any of the 1949 Conventions or of the Protocol, and thus explicitly refers to breaches of the targeting rules in API. Paragraph 3646 of the *API Commentary* makes the point that the provision in Article 3 corresponded to the general principles of law on state responsibility, a view which is endorsed by the International Law Commission (ILC) in its *Commentary* to Article 7 of the Draft Articles on State Responsibility, 2001, para. 4.

51 For a more detailed discussion of compensatory arrangements, see *API Commentary*, paras 3652–3659.

taken,[52] that the claimants have suffered loss meriting the award of compensation, that this loss was caused by the failure to take precautions[53] and that the case demands the award of compensation.

If the injury to civilians and/or damage to civilian objects was caused by a technical malfunction of the equipment, such as faulty software, a manufacturing defect or the erroneous insertion of data during mission preparation, complex issues are likely to confront any attempt to ascribe individual responsibility. Military personnel who act negligently will be subject to their military discipline code, while available action against negligent civilians will depend on their employment contract. If, however, the error that has occurred is such that the incident cannot properly be described as a violation, the law of armed conflict will not require the payment of compensation.[54] Specifically, it would seem difficult to characterize the negligent manufacture of weaponry as a violation such as to form the basis for a possible claim for compensation under Article 91.[55] Whether in a particular case a claim would lie under product liability law would depend on the terms of the particular legislation of the relevant state and on the ability of the claimants to bring the claim within the jurisdiction of that state's civil law courts. Such issues lie outside the scope of the present article.

Does remote attack amount to a legally significant change in the conduct of warfare?

Remoteness of attack would be legally significant were it to render rules of targeting inoperable, or to render it impossible to allocate criminal responsibility for

52 Note, for example, the decision of the Eritrea-Ethiopia Claims Commission, partly based on adverse inferences, reinforcing the conclusion that not all feasible precautions were taken by Eritrea in its conduct of air strikes on Mekele on 5 June 1998 and finding Eritrea liable for the resulting deaths and injury to civilians and damage to civilian objects, reflected in Eritrea-Ethiopia Claims Commission, Partial Award Decision, *Central Front, Ethiopia's Claim 2*, 28 April 2004, para. 112, available at: http://www.pca-cpa.org/showpage.asp?pag_id=1151.

53 'Compensation can only be awarded in respect of damages having a sufficient causal connection with conduct violating international law . . . The degree of connection may vary depending upon the nature of the claim and other circumstances'; Eritrea-Ethiopia Claims Commission, *Decision Number 7*, para. 7, available at: http://www.pca-cpa.org/showpage.asp?pag_id=1151. Later in the same decision, the Commission determined that the necessary connection is best characterized as 'proximate cause' and that in deciding whether that test is met the Commission would consider whether the relevant event should have been reasonably foreseen by an actor committing the international delict in question; *ibid.*, para. 13. It would be for an adjudicating court, tribunal, or commission to determine, in the light of its remit, whether a similar approach should be adopted in determining whether a sufficient causal relationship exists between a failure to take precautions and ensuing injury, damage, or loss.

54 Compensatory payment may, however, be made on an *ex gratia* basis, such as reportedly occurred following the attack of the Chinese Embassy in Belgrade by US aircraft operating with NATO on 7 May 1999; see Kerry Dumbaugh, 'Chinese Embassy bombing in Belgrade: compensation issues', in *CRS* Report for Congress, available at: http://congressionalresearch.com/RS20547/document.php.

55 See T. Gillespie and R. West, above note 31, citing A. Myers, 'The legal and moral challenges facing the 21st century Air Commander', in *Royal Air Force Air Power Review*, Vol. 10, No. 1, Spring 2007, pp. 76–96, for the view that the responsibility of designers is discharged 'once the UAS [unmanned aerial system] has been certified by the relevant national air authority'; T. Gillespie and R. West, *ibid.*, p. 7.

https://doi.org/10.1017/S1816383112000719 Published online by Cambridge University Press

wrongful acts or to adjudge whether compensation is payable for attacks that have unsatisfactory consequences.

There are, as we have seen, kinds of remote attack that do not pose such challenges. Thus, when a remotely piloted aerial vehicle is used to attack a target, the role of the remote pilot, usually referred to as the operator, mirrors that of a pilot of a manned aircraft such that targeting law rules can be applied in the same or a similar way, such that criminal liability could lie against the operator, say, in respect of a deliberate attack on civilians and compensation liability could be assessed and decided upon as in the case of an attack using a manned platform.

Moreover, in a sense, man has sought to fight from a distance since the earliest times. Concerns as to the ethics of such developments also date from ancient history.[56] The trebuchet, cannon, crossbow and longbow, artillery, bombardment from the air, and remotely piloted UAVs can all be regarded as technologically more refined methods of delivering offensive force against the enemy while incurring relatively less risk for one's own forces. This notion of seeking to protect oneself while placing the enemy at enhanced risk is of course central to many methods of warfare, which suggests that remoteness of the operator, per se, does not constitute a qualitative, and thus legally significant, change from what has gone before.[57] Perhaps the common thread here is that responsibility for attack decisions could always be readily ascribed at the personal, command and national levels. There will frequently be complications, for example where personnel from one nation on detached duty undertake attacks using platforms belonging to a state other than their own, either within a coalition or otherwise;[58] but those complications do not alter the fact that the person who ordered the attack, and the individuals who carried it out, can be identified and thus responsibility in the senses discussed in this article can be ascribed. Increasing the distance between the attacking individual and the scene where the destruction occurs does not, of itself, seem to change that. Rather, the issue seems to have more to do not so much with distance as with depersonalization altogether.

The anonymity or potential anonymity of a cyber attacker, the impossibility for the affected party to establish whose wrongful act caused an autonomous platform, say, to attack a civilian compound instead of a military objective, are examples of the sorts of circumstances in which we can say that these forms of remote attack would be starting to pose challenges for the law of targeting.

So let us consider autonomous attack technology a little further. If the platform belongs to and is operated by the armed forces of a state, that state will, it is suggested, have similar responsibility for what that piece of equipment does in the

56 The criticism by Idomeneus of the bow was that 'my way is not to fight my battles standing far away from my enemies'; Homer, *Illiad*, 13.262–3. O'Connell comments that the bow did not fit with the confrontational image that was the essence of heroic warfare; Robert L. O'Connell, *Of Arms and Men: A History of War, Weapons and Aggression*, Oxford University Press, Oxford, 1989, p. 48. Perhaps our ethical misgivings about some aspects of remote warfare have their origins in the Homeric notion of heroic warfare.

57 B. J. Strawser, above note 31, p. 343.

58 See Article 6 of the ILC Draft Articles on State Responsibility, 2001, available at: http://untreaty.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf, and note para. 3 of the associated commentary.

https://doi.org/10.1017/S1816383112000719 Published online by Cambridge University Press

battle space to its responsibility for the death, injury or damage caused, for example, by a missile or bomb fired using more conventional, manned technology. In other words, Article 91 of API will determine whether there is a legal obligation to compensate, and the state will retain the discretion whether to make an *ex gratia* payment in circumstances where no legal liability can be, or has been, established.

Some may seek to conclude from this that if, for whatever reason, a platform autonomously decides to make civilians or civilian objects the object of attack that would prima facie constitute a breach of, respectively, Articles 51(2) or 52(1) of API and would thus constitute a violation for the purposes of Article 91. The alternative view, which the author prefers, would take into account the design of the controlling software, the data fed into the mission control equipment, the settings applied to the algorithm-based technology, and any other information that would demonstrate what the persons planning and commanding the mission intended that the machine should attack. According to this alternative view, the 'object' of an autonomous attack consists of the object(s) and/or person(s) that the target recognition equipment was designed or intended to engage. According to this latter view, the machine is using its autonomous capability to achieve the object, or purpose, set for it by those individuals in charge of the mission, with the implication that liability to compensate will only be established under Article 91 if it can be shown that those planners and commanders had as their object of attack the protected persons or objects.

Where personal responsibility for erroneous autonomous attack is concerned, it would seem sensible to conclude that individuals will generally be responsible for their own actions in relation to the autonomous platform, its navigation, and its offensive operation.[59] If an individual were deliberately to configure the autonomous target acquisition software with the intention that the platform would target civilians and/or civilian objects, it follows that that would amount to a war crime in just the same way as using conventional capabilities with a similar intent would be.[60] If a failure to take required precautions, however, causes an erroneous autonomous attack a war crime is unlikely to be established; compensation may be payable if the requirements for establishing liability under Article 91 can be established; and individuals responsible for the failure to take precautions may be disciplined, for example on the basis of negligent performance of duties, to the extent this is provided for in applicable armed forces discipline legislation or in the contract of civilian employment.

Conclusion

The tentative conclusion that emerges from this discussion is that the established framework, whether in respect of war crimes, liability to compensate or domestic armed forces or civilian employment discipline, should be capable of being applied,

59 Consider, however, paragraph 5.32.9 of the UK Manual summarized above at note 42.
60 Whether proceedings on such a basis would be viable would, as always, depend on the available evidence.

https://doi.org/10.1017/S1816383112000719 Published online by Cambridge University Press

and therefore ought in fact to be applied, in the event of erroneous autonomous attacks. Persons who, in an international armed conflict, use autonomous technology deliberately to undertake unlawful attacks thereby breach the law of armed conflict as do those who use more conventional weaponry to like purpose. The fact that a machine is designed to act autonomously does not absolve those who give orders for the mission, those who plan the mission and those who take the necessary steps to enable the mission to be undertaken of responsibility for their own actions, and it is in the actions of those individuals that the basis for any criminality and liability to compensate is likely to be found.

Suggestions that criminal proceedings be taken against the machine are currently grounded in fiction. However, as notions of artificial intelligence (AI) continue to mature, it is conceivable that a point will arise at which human involvement is so remote, in a causal sense, from the decision to attack that commanders and planners can no longer sensibly be held accountable. In the author's view, we have not got to that point yet, but as technology becomes more complex and as decision-making relies increasingly on AI and less and less on human perception and judgement, the focus for responsibility may be expected to shift from planners and commanders to software engineers and the robots they beget.

https://doi.org/10.1017/S1816383112000719 Published online by Cambridge University Press