This is a repository copy of *Cyber Warfare and the Status of Anonymous under International Humanitarian Law*.

White Rose Research Online URL for this paper:
http://eprints.whiterose.ac.uk/109876/

Version: Accepted Version

Article:
Buchan, R. (2016) Cyber Warfare and the Status of Anonymous under International Humanitarian Law. Chinese Journal of International Law, 15 (4). pp. 741-772. ISSN 1540-1650

https://doi.org/10.1093/chinesejil/jmw041

This is a pre-copyedited, author-produced version of an article accepted for publication in Chinese Journal of International Law following peer review. The version of record Russell Buchan Cyber Warfare and the Status of Anonymous under International Humanitarian Law Chinese Journal of International Law (2016) 15 (4) is available online at: https://doi.org/10.1093/chinesejil/jmw041.

Reuse
Items deposited in White Rose Research Online are protected by copyright, with all rights reserved unless indicated otherwise. They may be downloaded and/or printed for private study, or other acts as permitted by national copyright laws. The publisher or other rights holders may allow further reproduction and re-use of the full text version. This is indicated by the licence information on the White Rose Research Online record for the item.

Takedown
If you consider content in White Rose Research Online to be in breach of UK law, please notify us by emailing eprints@whiterose.ac.uk including the URL of the record and the reason for the withdrawal request.

eprints@whiterose.ac.uk
https://eprints.whiterose.ac.uk/

Cyber Warfare and the Status of Anonymous under International Humanitarian Law

Russell Buchan*

Abstract

Since its emergence in 2003 Anonymous has become an increasingly prominent actor on the international stage. Anonymous is an online collective comprising like-minded individuals that commit cyber-attacks against state and non-state actors that are allegedly involved in the abuse of fundamental human rights. In recent years Anonymous has demonstrated a preparedness to commit cyber-attacks against parties to an armed conflict and the cyber-attacks launched against Israel during its 2014 armed conflict with Hamas are such an example. Using Anonymous's cyber-attacks against Israel as a lens, this article evaluates the status of online groups under international humanitarian law when they become embroiled in armed conflict and in particular under what circumstances members of these groups can be made the object of attack under the laws of targeting.

I. Introduction

1. Anonymous is an online collective that emerged in 2003 on a website known as *4chan*, which acts as a discussion board for individuals that wish to express and discuss anarchist ideas. Anonymous projects itself as a network of like-minded individuals that utilizes cyberspace for the purpose of protest. The members of this online community – which are known colloquially as Anons – discuss issues of contemporary concern, agree upon certain goals and then commit cyber operations against particular individuals or organizations for *lulz*, an adjective used to describe cyber conduct that is designed to derive entertainment at the expense of others whilst also raising awareness of the cause. Although the specific goals and objectives of Anonymous vary, the central objective of this group is the defence of fundamental human rights such as the right to liberty, freedom of expression and freedom of association. After members of the group agree to act in defence of a specific cause they debate

* Senior Lecturer in Law, University of Sheffield, UK. Contact: r.j.buchan@sheffield.ac.uk.

possible targets and, once a target is selected, discuss the cyber vulnerabilities of that target and determine which cyber operation should be utilized to cause the desired disruption or damage (whether it be website defacement, a Distributed Denial of Service (DDoS) attack, modifying or deleting data, exfiltrating and leaking sensitive information etc.). Members intending to launch a cyber-attack will then either acquire or develop the required computer malware themselves or particularly skilled members of the group will acquire or develop the malware for them.[1]

2. In its early years Anonymous gained notoriety by committing cyber-attacks against private corporations such as PayPal, MasterCard and Sony. Since then Anonymous has also committed cyber-attacks against the United States (US) Central Intelligence Agency (CIA) and the North Atlantic Treaty Organization (NATO) as well as governments allegedly involved in violent attacks against pro-democracy protesters in Tunisia, Libya and Uganda during the Arab Spring.

3. The activities of Anonymous became more serious when in November 2012 Israel launched Operation Pillar of Defense and intervened militarily in Gaza in order to deter and suppress missile fire from Hamas. As the number of civilian casualties in Gaza grew, Anonymous "declared cyber war on Israel's cyberspace" and "call[ed] upon our brothers and sisters to hack, deface, hijack, database leak, admin takeover, and DNS [domain name server] terminate the Israeli cyberspace by any means necessary". [2] In particular, members of Anonymous launched DDoS attacks against Israeli government websites. Technologically, however, these cyber-attacks were unsophisticated and "[t]he impact on the multiple targets in Israel, therefore, was minimal".[3]

4. In July 2014 Operation Protective Edge was launched and Israeli military forces were again deployed into Gaza as relations between Israel and Hamas deteriorated. As the humanitarian crisis in Gaza worsened Anonymous released a YouTube video "calling upon the Anonymous collective … to wage cyber war against the state of Israel",[4] with the objective of "systematically removing

---

1 For a detailed discussion of Anonymous and its activities, see Parmy Olsen, We are Anonymous: Inside the Hacker World of LulzSec, Anonymous and the Global Cyber Insurgency (2012); Gabriella Coleman, Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous (2015).

2 See the YouTube video posted by Anonymous entitled 'Anonymous #OpIsrael', posted on 17 March 2012 (https://www.youtube.com/watch?v=q760tsz1Z7M).

3 Bradon Valeriano and Ryan C. Maness, Cyber War versus Cyber Realities: Cyber Conflict in the International System (2015) 171.

4 YouTube video posted by Anonymous entitled "Anonymous: Message to Israel and Palestine", 19 July 2014

you [Israel] from the Internet".[5] On this occasion Anonymous's cyber-attacks were far more sophisticated, sustained and widespread. Online accounts belonging to senior Israeli public officials were hacked and their confidential details published on the internet[6] and acts of website defacement were also committed against various government websites such as the Ministries of Education and Finance, which involved replacing homepages with graphics, slogans and auto-playing audio files that depicted Israel as a brutal and violent repressor of Palestine.[7] Moreover, large Botnets were used to launch DDoS attacks against several hundred Israeli government websites, forcing many of them offline.[8] This included the websites of the Prime Minister's Office, Tel Aviv Police Department, the Ministry of Justice and the Bureau of Statistics and also, importantly, militarily significant websites such as those belonging to the Israeli Defence Force and Mossad (the Israeli Secret Service).[9]

5. To date, there has been no academic discussion of the status of Anonymous under international humanitarian law or, more specifically, whether the conduct of its members during the 2014 armed conflict between Israel and Hamas meant that they could be made the object of attack according to international humanitarian law rules on targeting. This lacuna in international law literature is especially concerning given that more recently Anonymous has further demonstrated its preparedness to become embroiled in armed conflict. In the wake of the November 2015 Paris terrorist attacks Anonymous declared "war on ISIS", which is a terrorist organization that claimed responsibility for

---

(https://www.youtube.com/watch?list=UUJ7eFTLJArvkgDBae1hbllw&v=iyQA3zMg7ZQ).

5 YouTube video posted by Anonymous entitled "Anonymous #OpSaveGaza Israel Leaks", 22 July 2014 (https://www.youtube.com/watch?v=-5HEzYoocGM).

6 David Gilbert, #OpSaveGaza: Anonymous Continues Cyber-Campaign Knocking Israeli Ministry of Defence Website Offline, International Business Times, 21 July 2014 (www.ibtimes.co.uk/opsavegaza-anonymous-continues-cyber-campaign-knocking-israeli-ministry-defence-website-offline-1457580).

7 Mary-Ann Russon, #OpSaveGaza: Anonymous Takes Down 1,000 Israeli Government and Business Websites, International Business Times, 18 July 2014 (www.ibtimes.co.uk/opsavegaza-anonymous-takes-down-1000-israeli-government-business-websites-1457269).

8 A Botnet describes a network of private computers infected with malware and controlled as a group without the owner's knowledge. Hijacked computers are often referred to as zombies.

9 David Gilbert, Anonymous Continues Cyber-Attacks on Israeli Government Websites Knocking Mossad and IDF Offline, International Business Times, 4 August 2014 (www.ibtimes.co.uk/anonymous-continues-cyber-attacks-israeli-government-websites-knocking-mossad-idf-offline-1459689).

the attacks in Paris and which is based largely in Syria and Iraq and is involved in a series of non-international armed conflicts with states such as Syria, Iraq, Russia and the USA, and warned ISIS to "expect massive cyber attacks" in the near future.[10] Furthermore, we are now witnessing the emergence of other online groups that are prepared to commit malicious cyber operations against parties to an armed conflict.[11] A better understanding of the status of such groups under international humanitarian law and the individuals that participate within them is therefore both timely and necessary.

6. This article is structured as follows. Section II provides some preliminary remarks relating to the difficulties in classifying the armed conflict between Israel and Hamas. Section III assumes that Israel and Hamas were involved in an international armed conflict and examines whether Anonymous can be regarded as an organized armed group belonging to a party to the conflict. Section IV instead assumes that Israel and Hamas were engaged in a non-international armed conflict and considers whether Anonymous and Israel were involved in a parallel yet separate non-international armed conflict. With sections III and IV concluding that members of Anonymous were properly regarded as civilians regardless of whether Israel and Hamas were engaged in an international or non-international armed conflict, section V assesses whether the cyber-attacks committed by members of Anonymous amounted to direct participation in hostilities and, if so, whether they could be directly targeted even though they were located outside of the conflict zone. Section VI offers some concluding remarks relating to the application of international humanitarian law to cyber conflict.

II. Classification of armed conflict between Israel and Hamas

7. International humanitarian law applies different regulatory frameworks depending upon whether an international or non-international armed conflict is occurring. In short, the rules applicable during international armed conflict are

---

10 Andrew Griffin, Anonymous War on ISIS: Online Activists Claim to have Foiled Terror Attack on Italy as Part of "Operations ISIS", The Independent, 28 December 2015 (www.independent.co.uk/life-style/gadgets-and-tech/news/anonymous-war-on-isis-online-activists-claim-to-have-foiled-terror-attack-on-italy-as-part-of-a6788001.html). The full quotation from Anonymous was: "We will launch the biggest operation ever against you. Expect massive cyber attacks. War is declared. Get prepared".

11 Ghost Security Group for example has also committed various cyber-attacks against ISIS. BBC News, Ghost Security Group: "Spying" on Islamic State Instead of Hacking Them, 23 November 2015 (www.bbc.co.uk/news/blogs-trending-34879990).

far more developed than those in non-international armed conflict.[12] Although a number of the rules applicable during international armed conflict are now becoming, via customary international law, also applicable during non-international armed conflict,[13] these legal frameworks are nevertheless distinct and "different rules apply to these different situations".[14] For this reason, it continues to be important to determine whether a particular incident of hostilities amounts to an international or non-international armed conflict (or, potentially, neither).

8. International lawyers have long disagreed over whether the violence between Israel and Hamas constitutes an international or non-international armed conflict. An international armed conflict is defined as "recourse to armed force between states" whereas a non-international armed conflict describes "protracted armed violence between governmental authorities and organised armed groups or between such groups within a state".[15] According to the *Tadić* definition, a non-international armed conflict only comes into existence when there is protracted armed violence between a state and an organized armed group (or between such groups) "within a state". Importantly, since *Tadić* state practice has extended the definition of non-international armed conflict to include protracted armed violence between a state and an organized armed group that operates from territory that is located outside of the state that is party to the non-international armed conflict.[16]

9. In light of Hamas's rocket fire into Israel and Israel's subsequent military intervention in Gaza, it is incontrovertible that the violence occurring between Israel and Hamas in July 2014 was of sufficient intensity to satisfy the requirement of "armed force" within the definition of international armed

---

12 Greenwood explains that the rules applicable during times of non-international armed conflict are 'almost skeletal when compared with the rules applicable to international conflict'. Christopher Greenwood, The Law of War (International Humanitarian Law), in Malcolm Evans (ed.), International Law (2006), 807.

13 Prosecutor v Tadić, Judgment, IT-94-I-I, 15 July 1999, para 96ff.

14 United Kingdom, The Joint Service Manual of the Law of Armed Conflict (2004) section 3.1 "[T]here is still a distinction between the law relating to armed conflicts between states, known as international armed conflicts, and armed conflicts within the territory of a state, known as internal (or non-international) armed conflicts", section 1.9.

15 Prosecutor v Tadić, Jurisdiction Appeal, IT-94-1-AR72, 2 October 1995, para 70.

16 Hamdan v Rumsfeld, 548 US 557 (2006). For a general discussion, see Sandesh Sivakumaran, The Law of Non-International Armed Conflict (2012), 228-235.

conflict and also "protracted armed violence" within the meaning of non-international armed conflict.[17] Whether this violence was of an international or non-international character hinges upon whether Israel (a state) was engaged in an armed conflict with the state of Palestine or, instead, Hamas as an organized armed group.

10. There is little doubt that Hamas is, at a minimum, an organized armed group given that it is the elected authority in Gaza and possesses a structured military force. Whether Hamas is a political authority within the state of Palestine is obviously a more complex and controversial issue. Rather than grapple with this difficult question, this article will explore both possibilities - that Israel and Palestine were involved in an international armed conflict and, the alternative, that Israel and Hamas were engaged in a non-international armed conflict. This has the advantage of allowing for greater breadth of analysis, providing the opportunity to examine the status of online collectives such as Anonymous under international humanitarian law when they become embroiled in armed conflicts of different legal classifications.

III. Anonymous and international armed conflict

11. Under the law of international armed conflict it is only combatants and military objectives that are permissible objects of attack. Formally, the purpose of Article 4(A) of the Third Geneva Convention (GC III) is to delineate the criteria for determining who can be regarded prisoners of war (POW) under international humanitarian law but, importantly, it has become well accepted that this provision also provides the criteria for determining lawful combatancy during international armed conflict. Article 4(A)(1) provides that combatants include those members of the regular armed forces of a state. In addition, Article 4(A)(2) extends combatancy status to irregular armed forces that belong to a party to the conflict. The rationale for this provision is to extend the privileges associated with lawful combatancy to irregular forces such as the resistance movements that operated during the Second World War (the French resistance, Jewish resistance etc.) which, whilst not officially incorporated into the armed forces of a state, exhibited characteristics and performed tasks closely resembling such forces.[18] It is only those members of these groups that

---

17 For an overview of the intensity of the violence, see UN Office for the Coordination of Humanitarian Affairs, Occupied Palestinian Territory: Gaza Emergency Situation Report, 4 September 2014.

18 "The Hague Regulations and the Third Geneva Convention thus consider all members of armed forces to be combatants and require militia and volunteer corps, including organized resistance movements, to comply with four conditions in order for them to be considered combatants entitled to prisoner-of-war status. The idea underlying these definitions is that the regular

possess a "continuous combat function" that will qualify as combatants, which is defined as "repeatedly" engaging in conduct that amounts to direct participation in hostilities.[19]

12. In order for a group to qualify as an irregular force six requirements must be satisfied. These requirements derive from Article 4(A)(2) GC III. Four are explicitly identified by Article 4(A)(2), which are: (1) being commanded by a person responsible for his subordinates; (2) having a fixed distinctive sign recognizable at a distance; (3) carrying arms openly; and (4) conducting its operations in accordance with the laws and customs of war. An additional two requirements are inferred by Article 4(A)(2): (5) organization and (6) belonging to a party to the conflict.[20] How these legal rules apply to online collectives such as Anonymous will now be considered. Given their commonality, issues (1) and (5) will be considered together, as will issues (2) and (3).

Responsible command and organization

13. In *Tarčulovski* the International Criminal Tribunal for the Former

---

armed forces fulfil these four conditions per se and, as a result, they are not explicitly enumerated with respect to them". Commentary to Rule 4 of the International Committee of the Red Cross's Customary Study; Jean-Marie Henckaerts and Louise Doswald-Beck, Customary International Humanitarian Law (2005).

19 Nils Melzer, Interpretative Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law (2009), 35. What conducts amount to direct participation in hostilities is considered in detail below.

20 It has been suggested that there exists a seventh requirement to determining combatancy status – that the individual in question must not have a duty of allegiance to the opposing party in the international armed conflict. Determining whether a duty allegiance exists is a difficult task and in the context of this article it would require us to determine whether members of Anonymous owed a duty of allegiance to Israel. However, the duty of allegiance criterion is only relevant to determining whether a person can claim POW status; even if a duty of allegiance exists the person in question continues to retain combatancy status, meaning that he is entitled to participate in hostilities and also remains a permissible object of attack. This is significant in the context of this article because our focus is upon whether members of Anonymous can be regarded as combatants and thus permissible objects of attack under the law of targeting, not whether members of Anonymous can claim POW status if they fall into the power of the opposing party. Discussion of whether members of Anonymous owe a duty of allegiance to Israel is therefore unnecessary. On the duty of allegiance, see APV Rogers, Combatant Status, in: Elizabeth Wilmshurst and Susan Breau (eds.), Perspectives on the ICRC Study of Customary International Humanitarian Law (2007), 107.

Yugoslavia (ICTY) identified a series of indicative factors that can be used to determine whether a group is organized.[21] This case concerned whether an armed group was sufficiently organized for the purpose of determining the existence of a non-international armed conflict within the meaning of Common Article 3 to the Four Geneva Conventions. However, there is no reason why these factors cannot be utilized to determine whether a group can be considered organized for the purpose of an international armed conflict.[22] The factors the ICTY identified were: evidence of a command structure; evidence that the group can carry out coordinated operations; evidence pertaining to the logistical capacities of the group; evidence demonstrating that the group maintains a level of discipline and the ability to implement the basic obligations of international humanitarian law; and evidence illustrating the group's ability to speak with one voice.[23]

14. Importantly, these factors are regarded as indicative only; not all need to be present in order to conclude that a group is organized. Generally speaking, though, the more of these indicative features that are exhibited by the group the more likely it will be that the group will be regarded as organized. The exception is the requirement that the group is subject to responsible command, which Article 4(A)(2) specifically identifies as a legal requirement for members of a group to be regarded as combatants in an international armed conflict.

15. Can an online collective such as Anonymous be regarded as an organized group subject to responsible command? In her major study of Anonymous Olsen refers to this group as a "global cyber insurgency",[24] which is an interesting use of language indicating that this group exhibits a high degree of military-style organization.

16. With regard to the requirement that the group is subject to responsible command, the function of this criterion is to exclude from combatancy status rogue individuals that initiate private wars and which are not embedded within a broader command structure that is capable of ensuring respect for the laws and customs of war.[25] When deciding whether a group is subject to responsible

---

21 Prosecutor v Ljube Boškoski and Johan Tarčulovski, Judgment, IT-04-82-T, 10 July 2008, paras 199 – 203.

22 Peter Margulies, Networks in Non-International Armed Conflicts and Defining "Organized Armed Group", 89 International Law Studies (2013), 54.

23 Tarčulovski, above n. 21, paras. 199 – 203.

24 Olsen, above n. 1.

25 The Commentary to AP I explains that the term organized requires that "the fighting should have a collective character, be conducted under proper control and according to rules, as opposed to individuals operating in isolation with no corresponding preparation or training". Yves Sandoz, Christophe Swinarski and Bruno Zimmermann, Commentary on the Additional Protocols

command, what is important is that we are able to identify individuals within the group that are "capable of ensuring generally the execution of … orders, including, as far as possible, respect for the laws and customs of war".[26]

17. To determine whether Anonymous is subject to responsible command it is first necessary to understand the structure and composition of this group. Crucially, by design Anonymous does not possess a stable and identifiable membership. This is because members can come and go as they please – they simply choose to logon or logoff the discussion board where members of Anonymous meet (usually *4chan*) depending upon whether they want to raise an issue of concern or participate in the discussion of a particular concern. The ability of members to contact each other is therefore entirely dependent upon their mutual willingness to logon to the discussion board, which clearly inhibits the ability of members of the group to exercise authority over others.

18. Moreover, it is left to members of Anonymous to interpret the group's broad goals and objectives and for them to decide themselves how such objectives should be achieved and when action should be taken. In addition, when a group member commits a cyber-attack he can choose to ascribe the attack to Anonymous or instead claim responsibility for the attack himself or even refuse to disclose who is responsible for the attack altogether. If the individual does not ascribe responsibility for the cyber-attack to Anonymous then the group may never know that an attack has been carried out in its name. In this sense, "anyone can be part of it [Anonymous]. It is a crowd of people, a nebulous crowd of people, working together and doing things together for various purposes".[27] In other words, Anonymous is more akin to a movement that inspires its followers to act, rather than a coherent group with particular individuals directing and coordinating the activities of its members.

19. In recent years certain members of Anonymous have taken the lead in identifying potential targets and the cyber vulnerabilities of those targets and then sharing this information with others that are willing to participate in a cyber-attack. These lead members also provide considerable advice and guidance to other members about which cyber weapons should be used to commit the attack and also perform a key role in locating and developing the

---

of 8 June 1977 to the Geneva Conventions of 12 August 1949 (1987), 512.

[26] Respect for Human Rights in Armed Conflicts, Report of the Secretary-General, A/8052, 18 September 1970, para. 176.

[27] Olsen, above n. 1, 68. "[O]ne member or a small group of members can decide to engage in an online action that is derived from the Anonymous ethos; others in the collective are then free to join the action or not". Paul Rexton Kan, Cyberwar in the Underworld: Anonymous versus Los Zetas in Mexico, 8 Yale Journal of International Affairs (2013), 44.

malware that is needed in order for the attack to go ahead.[28] In addition, lead members have been responsible for making announcements on behalf of Anonymous, such as the YouTube video claiming responsibility for the cyber-attacks against Israel in July 2014, implying that Anonymous speaks with one voice.

20. This notwithstanding, such features do not produce leadership in the sense required by international humanitarian law. Although influential members may have emerged within Anonymous, given Anonymous's amorphous identity such individuals cannot authoritatively direct group members to act or abstain from acting in a certain way and in particular cannot streamline the group's activities in conformity with the laws of war. As Olsen explains, "there [is] no single leader pulling the levers, but a few organizational minds that sometimes pool together to start planning a stunt".[29] In fact, "Anonymous takes pride in being unstructured without a hierarchy or central authority."[30]

21. In relation to whether a group is organized more generally, international tribunals have provided more detailed guidance on the indicative factors pinpointed in *Tarčulovski*. The following features have all been identified as suggestive of a group that is organized: the existence of a headquarters;[31] wearing uniforms;[32] the assignment of tasks to individuals within the group;[33] the ability to procure, transport and distribute arms; recruiting new members;[34] and affording training to members of the group and taking disciplinary action against them.[35]

22. Applying these criteria, could it be argued that *4chan* is the headquarters of Anonymous in that it is the venue where members of Anonymous meet to discuss ideas and identify targets and where cyber weapons are either distributed or at least information is available about how to develop or where to find such weapons? The Guy Fawkes mask is usually displayed on websites that have been hacked by Anonymous as a way of claiming responsibility. Could this be viewed as akin to a uniform in the sense that it represents unity and symbolizes a sense of collective identity? Could Anonymous be regarded as having implemented a code of conduct on the basis that members are expected

---

28 Olsen, above n. 1, chapter 2.

29 Ibid., 58-59.

30 Kan, above n. 27, 44.

31 Prosecutor v Milosevic, Decision on Motion for Acquittal, IT-02-54-T, 16 June 2004, para. 23

32 Prosecutor v Limaj, Bala and Musliu, Judgment, IT-03-66-T, 30 November 2005, para. 123.

33 Ibid., paras. 100-101.

34 Ibid., para. 118.

35 Ibid., paras. 113-117.

to adhere to certain rules, such as that members must keep their real life identities anonymous, talking about the group is prohibited and that the media is not a permissible target for cyber-attack? Perhaps this code of conduct can also be regarded as being accompanied by a type of disciplinary procedure insofar as individuals alleged to have breached Anonymous's rules are ignored in or even prevented from entering Anonymous's chatrooms?

23. These features notwithstanding, if we recall that the underlying rationale of Article 4(A)(2) is to extend combatancy status to irregular forces that mimic traditional military units,[36] it becomes difficult to conclude that Anonymous possesses a headquarters, a uniform and a code of conduct accompanied by disciplinary procedures that are "characteristic of the military".[37] When combined with the fact that Anonymous is a loosely associated network of individuals bereft of responsible command, it is clear that this group cannot be considered organized for the purpose of Article 4(A)(2).

Fixed distinctive emblem and carrying arms openly

24. Distinction is a "cardinal principle" and "intransgressible rule" of international humanitarian law and provides that parties to an armed conflict must distinguish between combatants and civilians and between military objectives and civilian objects.[38] The requirements that members of a group must exhibit a fixed distinctive emblem recognizable at a distance and carry arms openly are derived from the principle of distinction because such features "help protect the civilian population by helping to distinguish military forces from the civilian population."[39] But these legal requirements were formulated in 1949 with the physical battlefield in mind, where combatants and civilians are visible to each other and thus capable of distinction. Is it possible for cyber groups that operate in a virtual domain to comply with such requirements?

---

36 The ICRC has suggested that there should be "no difference in the degree of organization" between armed forces of the state and non-state armed groups. Official Records of the Diplomatic Conference on the Ratification and Development of International Humanitarian Law Applicable in Armed Conflicts, Geneva (1974-1977) (1978), vol. 8, 204, para. 15.

37 The US has refused to accord POW status (and, by implication, lawful combatancy) to members of the Taliban in Afghanistan because this group "lacked the kind of organization characteristic of the military". US Department of Defense, Status of Taliban Forces under Article 4 of the Third Geneva Convention of 1949, 3 7 February 2002 (https://fas.org/irp/agency/doj/olc/taliban.pdf).

38 Legality of the Threat or Use of Nuclear Weapons, (Advisory Opinion) [1996] ICJ Rep 226, 257.

39 US Department of Defense, Law of War Manual (2015), 203.

25. It is often noted that when applying these provisions their "phraseology should be reasonably construed" in order to give effect to their purpose rather than their literal meaning.[40] For example, Dinstein contends that members of an organized group would still be regarded as combatants even if, whilst sleeping in camp, they are attacked by the enemy and fight back before putting on their uniforms. Dinstein stresses that "[t]he point is not whether combatants can be seen, but whether (if observed) they are likely to be mixed up with civilians".[41] Similarly, Dinstein explains that members of a group will not be deprived of combatant status because, during wintertime, their sidearms are inadvertently concealed by their coat. Instead, what is important is that they do not conceal their weapons in such a way as to create the false impression that they are civilians. The obligation is that "[h]e must carry his arms openly in a reasonable way, depending on the nature of the weapon and the prevailing circumstances".[42] The upshot of this purposive interpretation of Article 4(A)(2) is that in a situation "where there is no danger of deception or of the combatant being mistaken for a civilian, the need for an individual to wear a distinguishing emblem [and to carry arms openly] is irrelevant".[43]

26. With regard to cyber, because "CNAs [computer network attacks] effectively remove the appearance of the combatant-operator from the distinction equation", [44] it can be regarded as irrelevant as to whether combatants wear a fixed distinctive emblem recognizable at a distance when launching attacks in cyberspace or whether arms are carried openly. What is relevant however is if a person launches a cyber-attack and deliberately spoofs his Internet Protocol (IP) address to make it look as if it emanated from a civilian user domain. To confer combatancy status to such an individual would violate the kernel of Article 4(2)(A) because it would risk civilian users being identified as the source/perpetrator of the attack and who are then put in danger of being targeted in a counter-attack.[45] Similarly, a person that launches

---

40 Yoram Dinstein, The Conduct of Hostilities under the Law of International Armed Conflict (2016), 53.

41 Ibid. See also the Tallinn Manual, which explains that "the requirement only applies in circumstances which the failure to have a fixed distinctive sign might reasonably cause an attacker to be unable to distinguish between civilians and combatants, thus placing civilian at greater risk of mistaken attack"; Michael N. Schmitt (ed.), The Tallinn Manual on the International Law Applicable during Cyber Warfare (2013), 99.

42 Dinstein, above n. 40, 54.

43 Heather Harrison Dinniss, Cyber Warfare and the Laws of War (2012), 148.

44 Sean Watts, Combatant Status and Computer Network Attack, 50 Virginia Journal of International Law (2010), 440.

45 "CNAs [computer network attacks] routed through civilian servers or

a DDoS attack that is intentionally hidden and camouflaged amongst legitimate civilian operations would also be denied combatant status because this method of attack entangles civilian users within the hostile operation and puts them at risk of being counter-targeted. Note however that cyber operations that are designed to covertly implant malicious software in computer systems and networks (such as a Trojan horse) would not preclude the conferral of combatant status because the requirement to carry arms openly does not mean "visibly" because "[s]urprise is a factor in any war operation".[46] The nub of the issue is whether weapons are being carried (or rather concealed) treacherously in such a way that risks mixing up combatants and civilians.

27. Given Anonymous's use of IP spoofing software such as The Onion Router (Tor) and Visual Private Networks (VPNs) to mask the true source of its cyber-attacks and that this created the mistaken impression that they had emanated from civilian users, and that DDoS attacks were also used to flood target websites with requests from tens of thousands of zombied civilian computers, Anonymous cannot be regarded as having complied with the principle of distinction.

Compliance with international humanitarian law

28. Combatancy status confers a number of privileges upon combatants, which include: combatants cannot be prosecuted for (domestic) crimes committed during an armed conflict; if captured combatants are entitled to POW status; and, if detained as a POW, combatants must be released at the end of the armed conflict. However, persons will be deprived of combatant status and estopped from enjoying its associated privileges where their actions fail to comply with international humanitarian law. In the context of armed groups, what is required is that we look at the activities of the group and assess its record of compliance with international humanitarian law. If the group as a whole does not comply with international humanitarian law, members of that group cannot be regarded as combatants.[47]

29. In relation to the activities of Anonymous, the main question is whether the conduct of its members complies with the rules of targeting. A key feature of the law of targeting is that civilians and civilian objects must not be made the object of attack, where attack is defined as "acts of violence against the

---

programmed to appear as though they originated from civilian institutions may in fact run afoul of states' duty to bear arms openly in the attack." Ibid., 442.

46 Jean Picket, Commentary, III Geneva Convention Relative to Treatment of Prisoners of War of 12 August 1949 (1960), 61.

47 Dinstein, above n. 40, 60.

adversary, whether in offence or defence".[48] According to the Commentary to AP I, "[t]he term 'acts of violence' denotes physical force. Thus, the concept of 'attacks' does not include dissemination of propaganda, embargoes, or other non-physical means of psychological or economic warfare."[49] In order to constitute an attack the conduct in question must therefore produce violent consequences, notably death or injury to people or damage to physical property.

30. The question then is whether Anonymous's cyber operations against Israel amounted to attacks against civilians or civilian objects in violation of the law of international armed conflict. Certainly, a number of the Israeli websites targeted by Anonymous could be classified as civilian objects because their "nature, location, purpose or use" did not make "an effective contribution to military action".[50] Examples would include the websites belonging to the Bureau of Statistics and the Office of the Prime Minister. However, the cyber operations committed against these targets did not produce violent consequences. Instead, the cyber-attacks caused non-kinetic harm such as loss of functionality of computer systems and networks, website defacement and the exfiltration of electronic data. On this basis, Anonymous did not commit attacks against civilian objects in violation of international humanitarian law.

31. In normative terms, if the primary objective of international humanitarian law is to protect civilians from the damage and destruction incidental to warfare,[51] it is unsatisfactory that violent effects are the *sine qua non* of the definition of attack. In the Internet Age state and non-state actors are now heavily reliant upon computer systems and networks to perform their manifold activities and discharge their various responsibilities. As a result, even those cyber-attacks whose effects are confined to cyberspace, such as cyber-attacks

---

48 Article 49 AP I 1977. It has been contended that military operations more broadly must distinguish between combatants and civilians, as opposed to just attacks. However, both a literal interpretation of the relevant international treaties and state practice indicate that it is only attacks that must distinguish between combatants and civilians. See Michel N Schmitt, "Attack" as a Term of Art in International Law: The Cyber Operations Context, in: Christian Czosseck, Rain Ottis and Katharina Ziolkowski (eds.), Proceedings of the 4th International Conference on Cyber Conflict (2012), 289ff

49 Michael Bothe, Karl J. Partsch and Waldemar A. Solf, New Rules for Victims of Armed Conflict: Commentary on the Two 1977 Protocols Additional to the Geneva Conventions of 1949 (1982), 289.

50 Article 52(2) AP I 1977, which is also considered customary international law according to Rule 8, ICRC Customary Study, above n. 18.

51 See Theodor Meron, The Humanization of Humanitarian Law, 94 American Journal of International Law (2000), 239.

that cause computer systems and networks to cease functioning (and especially when these systems and networks sustain critical national infrastructure), can produce harm equivalent to physical violence and should be therefore regarded as attacks under international humanitarian law. By extension, where such cyber-attacks are committed against civilian computer networks and systems they should be considered unlawful under international humanitarian law.[52]

32. The Tallinn Manual, which is not a binding international law instrument but "examine[s] how extant legal norms appl[y] to this 'new' form of warfare",[53] adopts a similar albeit more moderate view. The majority of the International Group of Experts responsible for drafting the Tallinn Manual opine that a cyber-attack can be regarded as an attack under international humanitarian law providing it causes harm that "requires replacement of physical components", such as reinstallation of a computer's "operating system".[54] Put differently, the majority were of the opinion that a cyber-attack occurs where it causes damage that necessitates repair. The Tallinn Manual therefore also points towards a definition of attack that does not require the production of violent effects as traditionally understood.

Belonging to a party to the conflict

33. Members of organized groups are not combatants simply because they launch attacks against a party to an international armed conflict. To become combatants, members of an organized armed group must belong to a party of the armed conflict and thus commit attacks on behalf of that party. Without this affiliation to a belligerent party, such persons are instead civilians committing independent attacks during an international armed conflict that happens to be occurring between two opposing parties.

34. "Without any doubt, an organized armed group can be said to belong to a State if its conduct is attributable to that State under the international law of State responsibility."[55] Since the ICJ's 2007 decision in the *Bosnian Genocide* case it is fairly settled that the degree of factual control that a state must exercise over an organized group in order for its acts to be attributed to the state is that of "effective control",[56] a high threshold that would require the party to an armed conflict to "direct or enforce" the acts of the group.[57] There is no

---

52 See generally Dinniss, above n. 43, Chapter 4.

53 Tallinn Manual, above n. 41, 1.

54 Ibid., 108.

55 Melzer, above n. 19, 23.

56 Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnian and Herzegovina v. Serbia and Montenegro), Judgment of 26 February 2007, ICJ Reports (2007), para. 400.

57 Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. US),

suggestion that Hamas exercised effective control over the conduct of Anonymous in order for attribution to be made under the rules on state responsibility. The important question is whether Article 4(A)(2) embraces a more relaxed standard for determining whether a group belongs to a party to the conflict.

35. In the *Tadić* case the ICTY had to determine whether the acts of a paramilitary group were sufficiently affiliated to the state of Serbia in order to internationalize the otherwise non-international armed conflict that was occurring in the former Yugoslavia.[58] The ICTY concluded that there was sufficient affiliation because the acts of the paramilitary group could be regarded as belonging to a party to the conflict under Article 4(A)(2) GC III. In doing so, the ICTY explained that a group will belong to a party to the conflict where the state exercised "overall control" over the group, which was interpreted to mean that the state provided material assistance to the group (money, weapons etc) and also participated in the planning and coordination of its military operations.[59]

36. The requirement of overall control undoubtedly imposes a "less stringent" standard for determining whether a group belongs to a party to the armed conflict than that of effective control, the test for attribution under the rules on state responsibility.[60] However, the ICTY's requirement of overall control nevertheless requires the exercise of factual control by the party to the armed conflict over the group, which remains a burdensome threshold. There is no evidence to indicate that Hamas exercised overall control (or any control for that matter) over Anonymous.

37. The ICTY's requirement of control can be criticized however on the basis that it confuses the law of state responsibility and law of international armed conflict. Whether an armed conflict can be internationalized depends upon the law of state responsibility and this correctly requires factual control to be exercised by the state over the armed group. However, Article 4(A)(2) is part of

---

Judgment of 27 June 1986, ICJ Reports (1986), para. 115.

58 Prosecutor v Tadić, Judgment, IT-94-1-A, 15 July 1999.

59 "States have in practice accepted that belligerents may use paramilitary units and other irregulars in the conduct of hostilities only on the condition that those belligerents are prepared to take responsibility for any infringements committed by such forces. In order for irregulars to qualify as lawful combatants, it appears that international rules and state practice therefore require control over them by a Party to an international armed conflict and, by the same token, a relationship of dependence and allegiance of these irregulars vis-à-vis that Party to the conflict. These then may be regarded as the ingredients of the term 'belonging to a party to the conflict'", ibid., para 1537.

60 Prosecutor v Delalić, Judgment, IT-96-21-A, 20 February 2001, para 20.

international humanitarian law and in particular relates to whether an individual can be regarded as possessing POW or combatant status. The ICTY thus misuses Article 4(A)(2) as a legal means to internationalize the armed conflict and in doing so misinterprets the concept of "belonging" to require factual control to be exercised which, as I have said, is the crucial ingredient to establishing state responsibility. In fact, if one looks to the Commentary to Article 4 of the Third Geneva Convention it is clear that a group will belong to a party where there is a "'de facto' relationship' between the resistance organization and the party [to the conflict]", and that such a relationship "may find expression merely by tacit agreement".[61] Del Mar therefore rightly argues that determining whether an organized group "belongs to a party to a conflict" should not be based upon whether the state exercises (overall) control over the organized group but should instead focus upon "motivation or intention of the armed group and the reaction of the state concerned: is the armed group fighting for the state, and does the state – either expressly or tacitly – accept the group is fighting on its behalf?"[62] Clearly, this sets the threshold considerably lower than the ICTY's approach of overall control. Kolb adopts a similar view, arguing for a twofold approach to determining whether a group belongs to a party to the conflict; first, the group must express "support" or "allegiance" to the state party which, second, is then accepted either expressly or tacitly by the state.[63]

38. Even if the tacit agreement test represents an accurate interpretation of Article 4(A)(2) it will not result in Anonymous being regarded as "belonging" to Hamas. Whilst Hamas accepted and even endorsed the cyber-attacks committed by Anonymous - for example Hamas proclaimed "[m]ay God protect the spirit and mission of the soldiers of this electronic war"[64] – it is quite clear that Anonymous had not expressed support for or allegiance to Hamas when launching the attacks but was instead acting out of ideological protest against the impact of Israel's policies on Palestinians. For example, in its various public announcements Anonymous justified its cyber-attacks on the basis of Israel's "violation of international law and crimes against humanity … against Palestinian territories" and because of "the Israeli Defence Force's barbaric and inhumane actions in where they bombed, raided and disrupted

---

61 Jean de Preux, Geneva Convention Relative to the Treatment of Prisoners of War: Commentary (1960), 57.

62 Katherine De Mar, The Requirement of "Belonging" under International Humanitarian Law, 21 European Journal of International Law (2010), 111.

63 Robert Kolb, *Jus in Bello* (2003), 160.

64 Quoted in Spiegel: Online, Cyberkrieg: Hacker Starten Angriffe auf Israel, 7 April 2013 (www.spiegel.de/netzwelt/web/anonymous-hacker-greifen-israelische-seiten-an-a-892960.html).

Gaza".[65] As Del Mar contends, the tacit agreement formula "excludes those non-state actors who claim to be fighting for a just cause, but who have no agreement with a state party to the conflict that they are fighting on the state's behalf".[66] As a result, Anonymous cannot be regarded as belonging to Hamas within the meaning of Article 4(A)(2).

IV. Anonymous and non-international armed conflict

39. This section assumes that Israel and Hamas were engaged in a non-international armed conflict on July 2014. If this is the case then the question is whether Israel and Anonymous were in a parallel yet separate non-international armed conflict with Israel. As we have already seen, a non-international armed conflict comes into existence where a state and an organized armed group are engaged in protracted armed violence. Israel is unambiguously a state under international law but the more complex questions are whether Anonymous is (i) organized (ii) armed and (iii) engaged in protracted armed violence with Israel.

Organized

40. The criteria for determining whether a group can be considered organized for the purpose of a non-international armed conflict were identified by the ICTY in the *Tarčulovski* case and further interpreted in subsequent cases, all of which were set out in the previous section. After applying these criteria to Anonymous I concluded that this online group did not exhibit the requisite features to be regarded as organized.

Armed

41. It is generally accepted that "[t]he logical construction of 'armed' is that the group carries out "attacks", as that term is understood in IHL [international humanitarian law]".[67] As we saw in our discussion above, the prevailing view is that the concept of attack only includes those acts that produce violent effects - death or injury to people or damage to physical property. This would mean that the cyber-attacks perpetrated against Israel cannot be regarded as attacks under international humanitarian law and *ipso facto* Anonymous cannot be regarded as being armed.

Protracted armed violence

42. The hostilities between a state and an organized armed group must reach a

---

65 See above n. 2.

66 Del Mar, above n. 62, 112.

67 Michael N Schmitt, Cyber Operations and the Jus in Bello: Key Issues, 87

certain level of intensity before a non-international armed conflict comes into existence.

> Factors relevant to assessing intensity include for example the number of fighters involved; the type and quantity of weapons used; the duration and territorial extent of fighting; the number of casualties; the extent of destruction of property; the displacement of the population; and the involvement of the Security Council or other actors to broker cease-fire efforts. Isolated acts of violence do not constitute armed conflict. The intensity criterion requires more than, for example, a minor exchange of fire or an insignificant border clash. None of the factors identified above is necessarily determinative in itself. A lower level with respect to any one may satisfy the criterion of intensity if the level of another factor is high.[68]

43. While it is possible for protracted armed violence to occur on the basis of cyber conflict alone, such as where a cyber-attack disrupts computer systems and networks which sustain critical national infrastructure and result in significant physical damage (such as interfering with aviation systems that cause planes to crash), "[m]ost commentators share the view that the high threshold of violence that is required for the existence of a non-international armed conflict means that it is unlikely that an armed conflict would be triggered by cyber means alone".[69]

44. Turning to Anonymous, I have already noted that while the cyber-attacks may have caused disruption and inconvenience to Israel because its computer networks and systems were temporarily unavailable and not working as intended, no physical damage occurred. Moreover, the cyber-attacks provoked very little response from Israel other than taking domestic measures to restore the functioning of its computer networks as well as beefing up its cyber defences generally. On this basis, it cannot be concluded that Anonymous and Israel were engaged in protracted armed violence.

V. Anonymous and the notion of direct participation in hostilities

45. Section 3 concluded that if Israel and Hamas were engaged in an international armed conflict, those members of Anonymous that launched

---

International Law Studies (2008), 99.

68 International Law Association, The Hague Conference: Use of Force – Final Report on the Meaning of Armed Conflict in International Law (2010), 30.

69 Louise Arimatsu, Classifying Cyber Warfare, in: Nicholas Tsagourias and Russell Buchan (eds.), Research Handbook on International Law and Cyberspace (2015), 341.

cyber-attacks against Israel must be regarded as civilians. Section 4 concluded that if Israel and Hamas were involved in a non-international armed conflict, Anonymous did not amount to an organized armed group engaged in protracted armed violence with Israel and thus those members of Anonymous that committed cyber-attacks against Israel must be classified as civilians that have become embroiled in Israel's non-international armed conflict with Hamas.

46. The rules relating to the targeting of civilians are the same regardless of whether an international or non-international armed conflict is underway.[70] With regard to both of these legal frameworks, civilians are protected persons that enjoy immunity from direct targeting. However, whether it is during an international or non-international armed conflict, civilians become liable to direct targeting where they directly participate in hostilities.[71]

47. Notwithstanding the importance of the concept of direct participation in hostilities treaty law does not provide any guidance as to its definition and there has also been little consideration of what this concept means by states through their military manuals. In recent years certain courts have sought to grapple with the meaning of the notion of direct participation in hostilities - notably the Israeli Supreme Court[72] and the ICTY[73] - but such definitions remain vague

---

70 "[M]ost experts believe that the same customary international law rules govern targeting and attack in both IACs and NIACs. For example … the U.S. view [is] that the principles of distinction, precautions, and proportionality, among others, apply with full force in NIACs." Adil Ahmad Haque, The United States is at War with Syria (2016), EJIL: Talk! Blog for the European Journal of International Law, 2016 (www.ejiltalk.org/the-united-states-is-at-war-with-syria-according-to-the-icrcs-new-geneva-convention-commentary/).

71 That civilians can be directly targeted in international and non-international armed conflicts where they directly participate in hostilities is embedded in Common Article 3 to the Four Geneva Conventions, expressly mentioned in Article 51(3) Additional Protocol I and Article 13(3) Additional Protocol II and is undoubtedly representative of customary international law, see The Public Committee against Torture in Israel *et al* v. The Government of Israel et al, Supreme Court of Israel sitting as the High Court of Justice, Judgment, 11 December 2006, HCJ 769/02.

72 The Israeli Supreme Court considered that "all those persons [who] are performing the function of combatants would be civilians that are taking 'direct part in hostilities'". The Public Committee against Torture, ibid., para. 35.

73 "To take a 'direct' part in the hostilities means acts of war which by their nature or purpose are likely to cause actual harm to the personnel or materiel of the enemy armed forces." Prosecutor v Galic, Judgment, IT-98-29-T, 5 December 2003, para. 48. See also the Strugar case where the ICTY defined

and even exhibit diversity.[74]

48. Concerned at the ambiguity surrounding the concept of direct participation in hostilities the ICRC conducted a six-year process of informal research and expert consultation with the aim of clarifying the circumstances under which a civilian can be regarded as directly participating in hostilities. Importantly, the ICRC's Guidance "does not purport to change the law, but provides an interpretation of the notion of direct participation in hostilities within existing parameters".[75] This notwithstanding, upon publication the Guidance was heavily criticized, with many arguing that it adopted an "overly narrow interpretation"[76] of the concept of direct participation in hostilities and "fail[ed] to pay sufficient regard to military realities".[77] Most importantly, scholars claimed that the Guidance deviated sharply from state practice on the topic of direct participation in hostilities.[78] Nonetheless, in the years subsequent to its publication the ICRC's Guidance has gained "traction"[79] among states and is thus "becoming the authoritative guidance on defining and interpreting DPH [direct participation in hostilities] for the international community".[80] As such, the ICRC's Guidance will be employed in this article as an authoritative

---

direct participation in hostilities as "acts of war which by their nature or purpose are intended to cause actual harm to the personnel or equipment of the enemy's armed forces". Prosecutor v Strugar, IT-01-41-A, Appeals Chamber Judgment, 17 July 2008, para. 167.

74 Emily Crawford and Alison Pert, International Humanitarian Law (2015), 109-113.

75 Melzer, above n. 19, 6.

76 Michael N Schmitt, Deconstructing Direct Participation in Hostilities: The Constitutive Elements, 42 New York Journal of International Law and Politics (2010), 720.

77 Shane Darcy, Direct Participation in Hostilities, Oxford Bibliographies, 2016 (www.oxfordbibliographies.com/view/document/obo-9780199796953/obo-9780199796953-0137.xml?rskey=3jCnSY&result=50).

78 For criticism of the ICRC's Guidance on direct participation in hostilities see volume 42 (2010) of the New York Journal of International Law and Politics.

79 Jeremy Marsh and Scott L. Glebe, Time for the United States to Directly Participate, 1 Virginia Journal of International Law Online (2011), 20.

80 Ibid., 14. For example Professor Philip Alston, Special Rapporteur to the UN Human Rights Council on extrajudicial, summary or arbitrary executions, cited the Interpretive Guidance as the primary authority on what constitutes direct participation in hostilities in his study on targeted killings; Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions: Study on Targeted Killings, Human Rights Council, UN Doc A/HRC/14/24/Add.6 (2010), paras. 62-69.

statement on the meaning of the concept of direct participation in hostilities under international humanitarian law.

49. The ICRC's Guidance comprises three limbs, all of which must be satisfied in order to conclude that civilian conduct amounts to direct participation in hostilities. After I consider how these criteria apply to Anonymous's cyber-attacks, I will then examine the ICRC's determination that direct targeting is only permissible "for such time" that direct participation occurs, with a view to better understanding how this qualifier applies in the cyber context. My attention will then turn to analyzing whether civilians that directly participate in hostilities can be directly targeted even though this conduct is committed from outside of the physical zone in which the armed conflict is occurring.

V.A Threshold of harm

50. The ICRC Guidance provides that "[i]n order to reach the required threshold of harm, a specific act must be likely to adversely affect the military operations or military capacity of a party to the armed conflict or, alternatively, to inflict death, injury, or destruction on persons or objects protected against direct attack".[81]

51. If the effect of the conduct under scrutiny is to cause "harm of a specifically military nature" the threshold of harm is met "regardless of the quantitative gravity" of the adverse effects.[82] This does not just include death or destruction of military objects and personnel but also extends to "essentially any consequence adversely affecting the military operations or military capacity of a party to the conflict".[83] Usefully, the ICRC Guidance provides examples of how this limb applies to cyber-attacks. In the context of cyber the Guidance explains that "electronic interference with military computer networks could […] suffice, whether through computer network attacks […] or computer network exploitation".[84] In light of this, those cyber-attacks perpetrated against websites belonging to the Israeli Defence Force and Mossad would undoubtedly meet this requirement.

52. If the harm caused is not of a military nature the "specific act must be likely … to cause at least death, injury or destruction on persons or objects protected against direct attack".[85] Evidently, this category contains two conditions. First, the object of harm must be protected persons or objects, namely civilians or civilian objects. In relation to the cyber-attacks committed

---

81 Melzer, above n. 19, 47.

82 Ibid.

83 Ibid.

84 Ibid., 48.

85 Ibid., 49.

by Anonymous, I have already noted that civilian websites were targeted. Second, by relying on the definition of the concept of attack contained in Article 49 AP I, the ICRC concludes that it is only conduct that produces violent consequences against protected person or objects that will meet the requisite threshold of harm.

53. The ICRC justifies this approach on the basis that it strikes an appropriate balance between the principles of humanity and military necessity that underpin contemporary international humanitarian law. Where physical violence is inflicted upon protected people or property this can be "equated with the use of means or methods of warfare".[86] Even if inflicted against protected persons or property non-violent acts are regarded as causing the enemy mere inconvenience and disruption (as opposed to damage and destruction), which is not considered sufficiently serious to justify the use of military force against those committing that conduct.[87]

54. The ICRC's approach seems anachronistic in the cyber era where cyberspace is now an indispensable feature of everyday life. Given this dependency, a significant cyber-attack against important civilian cyber infrastructure can cause tangible damage as opposed to mere disruption and can thus be equated with the use of means or methods of warfare. Fundamentally, however, at present there is a lack of state practice to support such an interpretive reorientation of the ICRC's definition of harm. Given that the cyber-attacks committed by members of Anonymous against Israeli civilian computer systems and networks did not produce physical harm, they would fall below the threshold of harm that is required by international humanitarian law to determine that a civilian is directly participating in hostilities.

V.B Direct causation

55. For conduct to qualify as direct participation in hostilities the ICRC Guidance requires that in addition to the requisite threshold of harm being attained the conduct must directly cause that harm. According to the ICRC, "[i]n order for the requirement of direct causation to be satisfied, there must be a direct causal link between a specific act and the likely harm to result … from that act".[88]

56. This requires that we distinguish between specific hostile acts on the one hand and contributions to the "general war effort" or to "war sustaining

---

86 Ibid., 50.

87 See further Nils Melzer, Keeping the Balance between Military Necessity and Humanity: A Response to Four Critiques of the ICRC's Interpretive Guidance on the Notion of Direct Participation in Hostilities, 42 New York Journal of International Law and Politics (2010), 862.

88 Melzer, above n. 19, 51.

activities" on the other.[89] Whereas the former satisfy the test for direct causation the latter do not. In short, the Guidance distinguishes "between direct and indirect causation of harm".[90] In this context "direct causation should be understood as meaning that the harm […] must be brought about in one causal step",[91] such as pulling the trigger of a gun or detonating a bomb.

57. In many situations cyber-attacks will satisfy the direct causation threshold. Take for example DDoS attacks, which have emerged as the weapon of choice for those seeking to cause harm to an adversary in cyberspace and which were widely used by members of Anonymous against Israeli websites in 2014. The Tallinn Manual explains that DDoS attacks provide an "unambiguous"[92] example of a cyber-attack that causes damage directly and thus meets the direct causation threshold. The reason for this is because once a Botnet containing a sufficiently large network of compromised computers is acquired all it takes is the touch of a computer key to instruct/command the Botnet to flood the target website with requests for information and cause the required damage.

58. This notwithstanding, because of the multi-layered structure of cyberspace combined with the increasingly complex algorithms that underpin cyber operations, in certain instances the damage caused by cyber-attacks will be ultimately indirect in effect. Consider the following extract:

> One of the most difficult-to-handle aspects of a cyberattack is that in contrast to a kinetic attack that is almost always intended to destroy a physical target, the desired effects of a cyberattack are almost always indirect, which means that what are normally secondary effects are in fact of central importance. In general, the planner must develop chains of causality – do X, and Y happens, which causes Z to happen, which in turn causes A to happen. Also, many of the intervening events between initial cause and ultimate effect are human reactions (eg, in response to an attack that does X, the network's administrator will likely respond in way Y, which means that Z – which may be preplanned – must take response Y into account). Moreover, the links in the causal chain may not all be similar character – they may involve computer actions and results, or human perceptions and decisions, all of which combine into some outcome.[93]

---

89 Ibid.

90 Ibid., 52.

91 Ibid., 54.

92 Tallinn Manual, above n. 41, 120.

93 William A. Owens, Kenneth W. Dam and Herbert S. Lin (eds.), Technology, Policy, Law, and Ethics Regarding US Acquisition and the Use of Cyberattack Capabilities (2009), 127.

In light of this, Turns concludes that the effects of more modern, complex cyber-attacks will often occur indirectly and are thus unlikely to "ever meet the requirement of direct causation for DPH [direct participation in hostilities], which suggests that civilians could engage in CW [cyber warfare] with impunity".[94]

59. The requirement of direct causation obviously sets the threshold for direct participation at a high level. It would mean for example that civilians such as those members of Anonymous that were involved in designing computer malware and/or disseminating malware to others cannot be regarded as directly participating in hostilities.[95]

60. An important caveat is that "the resulting harm does not have to be directly caused by each contributing person individually, but by the collective operation as a whole".[96] Thus, although some actions on their own may not directly cause the required threshold of harm they can satisfy the direct causation requirement if they constitute an "integral part of a concrete and coordinated tactical operation that directly causes such harm".[97] In this context the ICRC cites as examples "the identification and marking of targets, the analysis and transmission of tactical intelligence to attacking forces, and the instruction and assistance given to troops for the execution of a specific military operation".[98] Civilians who assist parties to an armed conflict by using the Internet to identify targets in the field or by relaying real-time intelligence about the opposing force's capabilities or movements, while not directly causing the resulting harm, would be regarded as engaging in conduct that forms a crucial (integral) element of the hostile act's successful execution and therefore satisfy the direct causation test. In relation those civilians that produce computer malware, although such conduct would be ordinarily regarded as indirectly causing harm it may, exceptionally, satisfy the test for direct causation where the civilian identifies the cyber vulnerabilities of a specific computer system or network and then manufactures bespoke malware and passes it to another with the knowledge that it will be used in a cyber-attack

---

94 David Turns, Cyber Warfare and the Notion of Direct Participation in Hostilities, 17 Journal of Conflict and Security Law (2012), 288.

95 According to the ICRC, "individual conduct that merely builds upon or maintains the capacity of a party to harm its adversary … is excluded from the concept of direct participation in hostilities … [examples of non-DPH] include scientific research and design, as well as production and transport of weapons and equipment". Melzer, above n. 19, 53 (footnotes omitted).

96 Melzer, above n. 87, 865.

97 Melzer, above n 19, 54-55.

98 Ibid., 55.

against the target's cyber vulnerability.

V.C Belligerent nexus

61. The final limb of the ICRC's test for determining direct participation in hostilities requires that the conduct under examination does not only directly cause the requisite degree of harm but "must also be specifically designed to do so in support of a party to an armed conflict and to the detriment of another".[99] Put differently, the conduct in question must be "so closely related to the hostilities conducted between parties to an armed conflict that they constitute an integral part of those hostilities".[100] The purpose of the belligerent nexus requirement is to therefore exclude conduct that is unrelated to the conflict, such as a civilian that exploits the chaos and lawlessness during an armed conflict to loot shops and residences as conduct not fulfilling the belligerent nexus requirement.

62. Did the cyber-attacks committed against Israel in 2014 satisfy the belligerent nexus criterion? The ICRC Guidance explains that "violent forms of civil unrest, the primary purpose of which is to express dissatisfaction with the territorial or detaining authorities"[101] do not possess a sufficiently close nexus to the armed conflict. According to the ICRC, although such conduct can cause harm to a party of the conflict it does not strictly speaking confer a benefit to the other party.

63. I have already noted above that the various public statements released by Anonymous indicate that its cyber war against Israel was an act of political protest against Israel's (perceived) violation of international humanitarian law and the adverse humanitarian impact of its policies on the Gazan population more generally. Although certain cyber-attacks may have directly caused military harm to Israel, crucially they were not specifically designed to support Hamas in its armed conflict with Israel.

64. Interestingly, the Tallinn Manual casts the belligerent nexus test more broadly and suggests that it is satisfied where the conduct in question "directly relates to the hostilities".[102] This suggests that "as long as there is some direct connection between the act and the hostilities, the civilian's action will be sufficient".[103] In contrast to the ICRC's Guidance the Tallinn Manual does not require that it be shown that the activity in question was specifically designed to

---

99 Ibid., 58.

100 Ibid.

101 Ibid., 63.

102 Tallinn Manual, above n. 41, 119.

103 Collin Allan, Direct Participation in Hostilities from Cyberspace, 54 Virginia Journal of International Law (2013), 188.

cause harm to one party *and* confer a benefit to another.[104] Evidently, the Tallinn Manual's framing of the belligerent nexus standard sets the bar lower than the ICRC's approach and could potentially encompass acts of political protest.

V.D "For such time"

65. If civilians directly participate in hostilities they can only be made the object of attack "for such time" that they engage in this activity.[105] The ICRC Guidance considers this to include not just when the hostile act is being committed but also during the period when measures preparatory to the execution of the specific hostile act are being undertaken and in the immediate aftermath of the operation.

66. In terms of directly targeting an individual before the hostile act is committed the key question is how extensive the preparation must be. The ICRC draws a distinction between conduct that is preparatory to "a specific hostile act" and conduct that is "aimed to establish the general capacity to carry out unspecified hostile acts";[106] in the former direct targeting is permissible whereas in the latter civilian protection remains and direct targeting is prohibited. The decisive issue is whether the preparatory conduct plays "an integral part of a specific act"[107] or, in other words, is undertaken with a "view to the execution of a specific hostile act".[108]

67. In the cyber context this would mean that an individual would not be liable to direct targeting when performing general and speculative acts of cyber reconnaissance/espionage in order to identify potential cyber vulnerabilities of an enemy. Such conduct would only render a civilian directly targetable when performed with the objective of identifying vulnerabilities in the computer systems and networks of an adversary in preparation for a specific cyber-attack. Similarly, a civilian that has written computer malware and is actively "zombie-ing" computers in order to develop a Botnet would be immune from direct targeting, unless of course the Botnet is being developed in preparation for a specific hostile act.

68. In relation to when an operation can be said to have ended (and thus the window for direct targeting closes) the ICRC contends that the individual must be "physically separated from the operation, for example by laying down, storing or hiding the weapons or other equipment used and resuming activities

---

104 Ibid., 189-190.

105 Article 51(3) AP I; Article 13(3) AP II.

106 Melzer, above n. 19, 66.

107 Ibid., 68.

108 Ibid., 66.

distinct from that operation".[109]

69. Although cyberspace is not a physical domain this standard of physical separation can be analogized to the cyber setting. For example, direct participation would end once a DDoS attack has been launched and the civilian goes offline or engages in different and unrelated cyber activity. If there is a delay between the launching of a cyber weapon and its activation (as would be the case with many malicious cyber operations, such as a logic bomb), direct participation will extend up to the point that the weapon is activated. As with civilians that lay improvised explosive devices on the physical battlefield, for example, direct participation ends upon activation and does not continue until the effects of the weapon have been felt, which may be many days, weeks, months or even years later.[110]

70. On the physical battlefield the ICRC's interpretation of the "for such time" qualifier arguably strikes an acceptable balance between the principles of military necessity and humanity. In particular, the ICRC's determination that direct targeting is only permissible when measures are being undertaken that are preparatory to a specific hostile act is acceptable from the perspective of military necessity because there is likely to be a certain period of time between a civilian engaging in preparatory measures and committing the attack. This means that that the opposing force will have a reasonable window of opportunity to identify the threat and react to it before the hostile act is launched. However, in an instantaneous environment like cyberspace cyber-attacks occur at lightening speed where malicious cyber operations can be conceived, the necessary tools acquired, the target identified, the act executed, and the operation terminated with the click of a mouse or the touch of a keyboard, all of which may only take a split-second.[111] By restricting direct targeting to only that timeframe when preparatory measures are being undertaken, opposing forces will have a very short window of opportunity to target the individual representing the threat.

---

109 Ibid., 67.

110 In the words of the Tallinn Manual, "[t]he majority of the International Group of Experts took the position that the duration of an individual's direct participation extends from the beginning of his involvement in mission planning to the point where he or she terminates an active role in the operation. In the example [of logic bombs] the duration of the direct participation would run from the commencement of planning how to emplace the logic bomb through activation upon command by that individual"; Tallinn Manual, above n. 41, 121.

111 "This is problematic in that many cyber operations last mere minutes, perhaps only seconds. Such a requirement would effectively extinguish the right to strike at direct participants." Schmitt, above n. 67, 102.

71. This problem is exacerbated considerably where civilians repeatedly commit cyber-attacks that amount to direct participation in hostilities, a likely possibility given the ease and speed at which cyber-attacks can be committed and the fact that individuals can perpetrate malicious cyber operations anonymously with little risk of being held to account. According to the ICRC's Guidance, where civilians repeatedly directly participate in hostilities they cannot be made the object of attack during intervals in their participation even though they form a deliberate and premeditated plan to repeatedly directly participate in hostilities. The ICRC justifies this conclusion on the basis that "[i]t prevents attacks on civilians who do not, at the time, represent a military threat".[112] For the ICRC, except for where civilians are preparing for the commission of a hostile act, committing that act or have yet to physically separate themselves from it, there is no pressing security threat to the opposing party and so military necessity cannot justify direct targeting. Instead, the party to the armed conflict must suspend targeting during lulls in participation and wait until preparatory measures are once again undertaken.

72. In the context of cyber, however, the ICRC's position would mean that even if on the basis of previous practice a party to the armed conflict can reliably predict that a civilian will commit future cyber-attacks, it can only directly target that person during each split-second that a new cyber-attack is being prepared, launched and concluded. This would provide very little or even no window of opportunity for the party to the armed conflict to directly target the individual and would mean that, in reality, it would have to withstand the repeated cyber-attacks. Such an approach is unsatisfactory from the perspective of military necessity because it prevents parties to an armed conflict from pursuing their legitimate security needs.[113]

V.E Cyberspace and the spatial scope of armed conflict

73. Cyberspace is a globally interconnected domain. As a result, it is possible and even likely that civilians utilizing cyberspace to directly participate in hostilities will do so far from where the armed conflict is physically taking place, perhaps even on the other side of the world. For example, the origins of the cyber-attacks committed against Israel in July 2014 were traced to geographical locations as far away as Asia and South America. An important question becomes whether a party to an armed conflict can make the object of attack civilians that are directly participating in hostilities even when they are far removed from the battlefield.

---

112 Melzer, above n. 19, 70.

113 Michael N. Schmitt, The Interpretive Guidance on the Notion of Direct Participation in Hostilities: A Critical Analysis, 1 Harvard National Security Law Journal (2010), 34ff.

74. With regard to international armed conflicts, international humanitarian law applies throughout the territory of the parties (states, usually) to the armed conflict, even to those areas where no fighting takes place.[114] Civilians that directly participate in hostilities from within this territory (such as launching cyber-attacks) can be directly targeted for such time that direct participation occurs.

75. Where a civilian commits hostile acts from the territory of a state that is not a party to the armed conflict, it is "well settled" that the law of neutrality applies.[115] The law of neutrality imposes an obligation upon non-belligerent (neutral) states to prevent their territory, which includes cyber infrastructure located upon their territory, from being used as a platform to commit conduct damaging to a party to an armed conflict.[116] Where a neutral state "significantly and systematically violates its neutral duties" it will be "treated as a co-belligerent" and will become a party to the armed conflict, with IHL applying throughout its territory.[117] Civilians that directly participate in hostilities from such territory can of course be directly targeted under international humanitarian law for such time that this participation occurs. In the absence of significant and systematic violations, such as where a state is unable despite its best efforts to put an end to damaging conduct emanating from its territory (which is a distinct possibility in the context of cyber where a state's

---

114 "As regards IAC [international armed conflict], it is generally accepted that IHL [international humanitarian law] applies to the entire territories of the States involved in such a conflict … There is no indication either in the 1949 Geneva Conventions and their Additional Protocols, or in doctrine and jurisprudence, that IHL is limited to the 'battlefield', 'zone of active hostilities' or 'zone of combat', which are generic terms used to denote the space on which hostilities are taking place", ICRC, International Humanitarian Law and the Challenges of Contemporary Armed Conflict (2015), 13.

115 Michael N Schmitt, Charting the Legal Geography of Non-International Armed Conflict, 90 International Law Studies (2014), 5.

116 Tallinn Manual, above n. 41, Rule 93. The focus of this article is upon the legality of targeting civilians that use cyberspace to directly participate in hostilities. However, it is prudent to note that a transiting state (providing it is a neutral state and thus not party to the armed conflict) is also under a duty to suppress damaging cyber conduct that originates in the territory of another state and is passing through its cyber infrastructure (its territory) *en route* to its intended target, which is a party to an international armed conflict. For a good discussion on the application of the law of neutrality to cyberspace see David Turns, Cyber War and the Law of Neutrality, in: Tsagourias and Buchan, above n. 69.

117 Tess Bridgeman, The Law of Neutrality and the Conflict with Al-Qaeda, 85 New York University Law Review (2010), 1200.

technological capabilities may be basic and rudimentary), the state will retain its neutral status and will not become a party to the armed conflict. Importantly, however, "a belligerent state may become entitled to use force in self-defence against enemy forces operating from the territory of that neutral state. Whether or not they are so entitled will depend on the ordinary rules of the *jus ad bellum*".[118]

76. Turning our attention to non-international armed conflicts, in a classic civil war scenario where government forces are engaged in protracted armed violence with an organized armed group, international humanitarian law applies throughout the territory of the state in question, even to those areas where no actual hostilities take place.[119] Thus, civilians that commit cyber-attacks from within the state and which amount to direct participation in hostilities would be liable to direct targeting for such time that direct participation occurs and wherever they are located within state territory.

77. In relation to a non-international armed conflict between a state and an organized armed group that operates from the territory of another state, international humanitarian law applies throughout the territory of the intervening state and also applies to "the whole territory on which the non-State party [the organized armed group] holds its (quasi-)military presence which enables it to carry out significantly intensive armed violence".[120] Civilians that commit cyber-attacks that rise to the level of direct participation in hostilities whilst within these territories would be liable to direct targeting under international humanitarian law for such time that direct participation occurs.[121]

78. The picture is more complex where civilians that directly participate in

---

118 UK Joint Service Manual, above n. 14, para. 1.43(a). "Should a neutral State fail to comply with this duty [its duty prevent its territory from being used in a manner harmful to a party to an armed conflict], either because it will not or cannot, the opposing belligerent may lawfully cross into neutral territory for the sole purpose of putting an end to its enemy's activities." Schmitt, above n. 115, 5.

119 "The geographical and temporal frame of reference for internal armed conflicts is … broad … [I]nternational humanitarian law continues to apply in the whole territory of the warring States or, in the case of internal conflicts, the whole territory under the control of a party, whether or not actual combat takes place there." Prosecutor v Tadić, Appeal, IT-94-1-A, 2 October 1995, para 69-70. The ICTR has reached a similar conclusion. Prosecutor v. Rutaganda, Judgment, IT-96-3-T, 6 December 1999, para. 6 ('[IHL] extends throughout the territory where the hostilities are occurring').

120 Claus Kress, Some Reflection on the International Legal Framework Governing Transnational Armed Conflicts, 15 Journal of Conflict and Security Law (2010), 266.

121 Schmitt, above n. 115, 15-16.

hostilities are located outside of the territory of the intervening state and the territory under the control of the organized armed group. As we have seen, in an international armed conflict the law of neutrality is designed to regulate this type of situation but there is a consensus that the law of neutrality does not apply to non-international armed conflicts.[122]

79. The ICRC adopts a restrictive view and argues that the permissive international humanitarian law rules relating to targeting do not apply to such individuals. Instead, the ICRC maintains that other international legal rules must be utilized to address the threat that they represent, notably those relating to the use of force in extra-territorial law enforcement operations and which are governed by international human rights law.[123] In such a scenario a state can only use force to the extent that it is necessary and proportionate in the circumstances.[124] For the ICRC, to allow international humanitarian law to extend to civilians that are directly participating in hostilities regardless of where they are located in the world "would lead to the acceptance of a legal concept of a 'global battlefield'" and that the potential ramifications of such a development would be "disturbing".[125]

80. However, the ICRC's approach is problematic because it would mean that individuals hostile to a party to an armed conflict could deliberately relocate to territory that is not under the control of a party to the armed conflict and thereby evade the reach of international humanitarian law.[126] This is particularly likely in cyber and, as hostilities increasingly migrate to the cyber domain, would be especially concerning.[127] "Distance cannot therefore be the primary

---

122 Michael Bothe, The Law of Neutrality, in: Dieter Fleck (ed.), Handbook of Humanitarian Law in Armed Conflict (2013).

123 ICRC Report, above n. 114, 15.

124 On the constraints imposed by international human rights law on the use of force see Human Rights Council, Specific Rapporteur Philip Alston on Extrajudicial, Summary or Arbitrary Executions, Study on Targeted Killings, UN Doc A/HRC/14/24?Add.6 (28 May 2010).

125 Ibid.

126 "[T]he extension of IHL [international humanitarian law] beyond the immediate geographical and temporal spheres of hostilities is necessary to prevent attempts by the Parties to an armed conflict to evade the reach of IHL by relocating individuals and directing operations away from the immediate sphere of hostilities." Noam Lubell and Nathan Derejko, A Global Battlefield: Drones and the Geographical Scope of Armed Conflict, 11 Journal of International Criminal Justice (2013), 74.

127 This concern relating to cyber is actually recognized by the ICRC, albeit only in a footnote; ICRC Report, above n. 114, 15 at footnote 13. Schmitt develops further this point on cyber; Schmitt, above n. 115, 17.

determinant for the applicability of IHL".[128] Instead, the better approach is to determine the status of the individual in question with a view to ascertaining whether there is a sufficiently close nexus between the individual's status and the armed conflict that is occurring. Put differently, "[w]hat is decisive is not where hostile acts occur but whether, by their nexus to the armed conflict, they actually do represent 'acts of war"'.[129] On this basis, members of the armed forces of a state would be clearly targetable wherever they are located, as would members of organized armed groups that perform a continuous combat function. In relation to civilians, the question is whether their conduct amounts to direct participation in hostilities. If it does then a sufficiently close nexus to the armed conflict would be established because, as we have seen, it is an essential ingredient of the test for direct participation in hostilities that the damaging conduct possesses a belligerent nexus. In such instances, civilians committing acts that amount to direct participation in hostilities can be directly targeted wherever they are in the world and for such time that they are engaging in that conduct.

VI. Concluding remarks

81. As exemplified by the cyber-attacks against Israel in 2014 and against ISIS in 2015, over the past several years Anonymous has demonstrated an increasing preparedness to become embroiled in armed conflict, as have other online groups. With these developments in mind, the objective of this article has been to examine the status of online groups such as Anonymous under international humanitarian law and to provide clarification.

82. This article has largely eschewed complex normative debates concerning the adequacy of existing international humanitarian law to regulate cyber conflict. Given the paucity of literature examining the status of Anonymous under international humanitarian law the primary purpose of this article has been to zero in on issues of *lex lata* – how does the law as it currently stands apply to online collectives? However, as this discussion has progressed it has become apparent that international humanitarian law was formulated long

---

128 Lubell and Derejko, above n. 126, 82.

129 Nils Melzer, Human Rights Implication of the Usage of Drones and Unmanned Robots in Warfare, Study, European Parliament, Directorate-General for External Policies, Policy Department, May 2013, 21. "The requirements for the applicability of IHL are: that an armed conflict is taking place, and that the operations in question are in fact between Parties to this armed conflict (nexus). The status of the individuals targeted or the attributes of the objects targeted, will then be relevant as to the lawfulness in accordance with IHL (as opposed to its applicability)." Lubell and Derejko, above n. 126, 83. For a similar view see Schmitt, above n. 115, 16.

before the potential for cyber warfare was contemplated and therefore provides a generally unsatisfactory legal framework that does not adequately take into account the unique features of cyberspace and the potential for this domain to be exploited for warlike purposes.[130] It goes without saying that if international humanitarian law is to retain its legitimacy and credibility – put differently, that international humanitarian law is to continue to attract compliance – it must keep apace with technological developments.

83. As cyberspace becomes ever more integrated into our daily lives and emerges as a more prominent means and method of warfare, we can expect to see states agitate in favour of reform of international humanitarian law – whether it be through the adoption of cyber-specific international agreements or state practice more generally – to ensure that it is able to more effectively address cyber conflict. The Tallinn Manual's progressive approach to applying international humanitarian law to cyber conflict is likely to act as a lightning rod around which future developments will converge.

---

130 "In the context of CNAs [computer network attacks], current applications of accepted legal standards for combatant status suffer similar detachment from reality." Watts, above n. 44, 446.