Tomasz Lewandowski
Adam Mickiewicz University Poznań

Can mouse clicking be seen as involvement in armed conflict? Some notes on the direct participation in hostilities in cyberspace

The history of the conduct of hostilities is tightly related with technological development. Over the centuries man has looked for more effective methods which could help him overwhelm his enemies without taking too many losses. Military technologies are particularly designed to put the man out of the loop. This is why gunpowder, sniper rifles, dynamite, rockets, torpedoes were invented. This is also how drones and robotics are developed. Contemporary armed conflicts rely greatly on new technologies which enable the participation of hostilities from a distance even by eliminating the human factor outside of the real battlefield. This phenomenon causes a lot of risks for the potential victims of modern armed conflicts. It also creates difficulties with the effective implementation of the international humanitarian law of armed conflicts (IHL) which was designed due to the collision between the art of warfare and issues of dignity and human compassion.

IHL is based on two groups of laws – the Geneva law and the Hague law. The first seeks to protect the victims of armed conflicts mainly civilians, while the latter provides guidelines on the conduct of hostilities mainly by the means and methods of warfare. The main foundation of this branch of international law is to distinguish persons who are legitimate, allowed to participate in hostilities and therefore permitted to being attacked and killed from those who are protected against attack and who therefore should not be taking a part in hostilities. Simply IHL is based on the differentiation between combatants and civilians. Civilians as all persons who are not members of the armed forces or party to the conflict nor participants are the most protected group of persons protected under IHL.

Again the history of warfare shows that the role civilians play in it is increasing rapidly. Moreover, it often takes the form of direct participation. Traditionally, direct participation in hostilities was associated with situation of civilians actually fighting against the enemy using similar methods as combatants. However, the new perspective of di-

stance hostilities enabled civilians to perform hostile acts without being present on the battlefield. As the consequence of new technologies development led by the invention of computers and the Internet, the concept of the battlefield has transferred from reality to cyberspace[1].

The Internet is an acronym of an inter-network which generally may be described as a worldwide computer network, also known as a network of networks[2]. The spread of the Internet encourages the development of technologies enabling individuals to perform almost every kind of activity. It has mostly a positive effect on world development and globalization; however there is also a less glamorous aspect of cybernetic human activity. The Internet enables people from all around the world[3] not only to communicate and share ideas but recently also to participate in hostilities. Governments seek to use the facilities given through such networks to obtain a military advantage on the battlefield. However, this process requires a level of knowledge and abilities greatly exceeding those of standard combatants. The special training of member states armed forces is really expensive and long, therefore it is obvious that the military needs a civilian factor to perform activities in cyberspace requiring IT skills of the best quality. The problem lies in the eventual identification of such activities as a form of direct participation in hostilities which "refers to conduct which if carried out by civilians, suspends their protection against the dangers arising from military operations"[4].

This article addresses the issues of direct participation in hostilities (DPH) in cyberspace. In the first part it discusses the impact of technological development on the activation of the civil factor during armed conflicts. It seeks to answer the question why civilians perform hostile acts through cyber network attacks. Then in the second part by analyzing the current practice of cyber conflicts it refers to the concept of direct participation in hostilities and its constituent elements (threshold of harm, direct causation, and belligerent nexus) at the cybernetic level. The third and final part examines the possibility of the loss of protection, in particular, it addresses the issues related to its temporal nature and the question of means and methods of attacking civilians involved in cyber warfare.

1 The vast array of public and private networks connecting computers and users all over the globe; D. E. Denning, P. P. Macdoran, *Grounding Cyberspace in the Physical World*, [in:] *Cyberwar: Security, Strategy and Conflict in the Information Age*, ed. A. D. Campen, Fairfax 1998, p. 119.

2 A. S. Tannenbaum, *Sieci komputerowe*, Gliwice 2004.

3 As of 2011 Internet World Stats, more than 2.1 billion people – nearly a third of Earth's population – use the services of the Internet.

4 N. Melzer, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law*, Geneva 2009, p. 12.

Civilians directly participating in hostilities

The customary rule states that civilians are not the object of any attack unless directly participating in hostilities[5]. Therefore it is obligatory to begin with defining civilians as all persons who are not or no longer either members of the armed conflicts of a party to the conflict or participants in a *levee en masse*[6]. Civilians take part in hostilities in different ways ranging from an indirect general contribution to war efforts to exact belligerent activities performed on the battlefield. Not all civilian behaviour can be qualified in a category of direct participation in hostilities in a context given by IHL. Such a qualification depends on the circumstances prevailing at the relevant time and place. Moreover, such a qualification does not affect a person's status, therefore a civilian cannot be transformed into a combatant simply by directly participating in hostilities. Civilians are not prohibited to take a part in hostilities, they are not however also permitted do so. However, there are situations in which civilians actually participate in hostilities and they do it really actively. I leave the topic of civilians performing a continuous combat function during non-international conflicts, I simply focus on the issue of civilians spontaneously deciding to actively participate in hostilities especially in cyberspace. They can be divided into two groups: private contractors working on behalf of belligerent armed forces[7]and freelancers – talented hackers working on their own behalf.

Cyberspace gives a great opportunity to perform different acts against the enemy. These include illegal exploration, hacking, cyber crimes, hacktivism, espionage, terrorism, warfare[8]. Civilians can do it intentionally or unintentionally. Intentional actors intend to compel an opponent to fulfil a national will, executed against an opponent's computer and software systems[9]. Unintentional cyber actors are civilians who unintentionally attack but affect national security and are largely unaware of the international ramifications of their actions[10]. This includes cyber infiltration, penetration of the defen-

5 J.M. Henckaerts, L. Doswald-Beck, *Customary International Humanitarian Law*, vol. I, Cambridge 2005.

6 N. Melzer, *op. cit.*, p. 30; *V.* ICTY, Prosecutor v. Blaskic, Case no. IT-95-14-T, Judgement of 3 March 2000, para. 180.

7 This group however is recruited, regardless of form, by the armed forces. Therefore, such an authorization of civilians direct participation in hostilities by state causes a transformation from civilian into a member of the armed forces/combatant status. *V.* Report DPH 2003 p. 4 f.; Report DPH 2004, p. 11 f., 14; Expert Paper DPH 2004, p. 8 ff.; Report DPH 2005, p. 74 ff and 80 f.; Background Doc. DPH 2005, WS VIII-IX, p. 17.

8 N. Solce, *The Battlefield of Cyberspace: The inevitable New Military Branch – The Cyber Force*, "Albany Law Journal of Science & Technology" 18 2008, p. 293, 301.

9 Therefore, if working under a government order they may be recognized as members of armed forces; *v.* D. Alford Jr., *Cyber Warfare: Protecting Military Systems*, "The Journal of Defense Acquisition University" no. 2, 2000, p. 105.

10 *Ibidem*.

ces of a system. Sometimes they can be influenced and manipulated by intentional actors to participate in cyber operations[11].

Civilians start to actively participate in hostilities motivated by different factors. The first group may be described as "harmless". It consists of users who do not intend to cause harm to a victim. Their motivations range from the simple will to perpetrate tricks, impress others, building a reputation, feelings of pleasure or a thrill, facing a challenge, possessing more knowledge and abilities[12]. The second group 'harmful' consists of users who intend on causing loss based on political or antisocial motives or getting financial goals[13]. A civilian may act against its own state or against the enemy state. In both cases he/she commits a crime. His/her will to engage in a hostile attack may be an effect of dissatisfaction with a particular action or policy of the government. Civilians may just wish to object, sure to draw attention to the problem, as well as to fight the unjust, according to his/her assessment behaviour of the State. Their reasoning is based mostly on humanitarian and fraternal causes. This type of behaviour is called hacktivism[14]. It includes Distributed Denial of Service Attacks mostly on government websites as well as publishing some manifestos on them, which may be accomplished with only one computer in a multitude of ways. The extensive computer games industry is not without influence on the issue. It has facilitated the creation of so-called virtual soldiers, specializing in virtual war performed through Massive Multiplayer Online Games (MMOG or MMO). Frequently addicted to the game, they will, if having suitable hacking skills, try taking a virtual part in real hostilities. Often unaware of the consequences of their actions they treat it as an exciting form of an entertainment[15]. Others take even more drastic measures. They are often inspired by nationalistic or anarchist motives and simply seek to terrify and destroy the enemy. It is even more "tempting when hackers have the power to participate on the international scene"[16] Despite these factors any civilian from teenage hacker to professional hacker taking part in criminal activity may have the skills necessary to create extensive damage to cyber infrastructure wherever in the world. Moreover, the danger arises when we take into consideration that any attack can be performed distantly and anonymously. Even the mere existence of such risk forces parties to a potential conflict to take measures to prevent and if necessary counter-attack.

---

11 *Ibidem*.

12 Examples of members of this group are pranksters and hackers.

13 Crackers, professional hackers (career criminals), hacktivists, cyber terrorists.

14 S. Wray, *Electronic Civil Disobedience and the World Wide Web of Hacktivism: A Mapping of Extra parliamentarian Direct Action Net Politics*, A paper for The World Wide Web and Contemporary Cultural Theory Conference, Drake University 1998.

15 This may be described as a video game syndrome.

16 C. Kirby, *Hacking with a Conscience is a New Trend*, "San Francisco Chronicle" 20th November 2000.

Direct participation in hostilities in cyberspace

As it has been already mentioned direct participation in hostilities is restricted to specific hostile acts. It is necessary to underline that the IHL interpretation of the notion of direct participation in hostilities covers actions taken by civilians during existing armed conflict both of an international and non-international character. To be interpreted as such under IHL it has also to meet three cumulative conditions. Firstly, "the act must be likely to adversely affect the military operations or military capacity of a party to an armed conflict or, alternatively, to inflict death, injury, or destruction on persons or objects protected against direct attack (threshold of harm). Secondly, there must be a direct casual link between the act and the harm likely to result either from that act, or from a coordinated military operation of which that act constitutes an integral part (direct causation). Lastly, the act must be specifically designed to directly cause the required threshold of harm in support of a party to a conflict and to the detriment of another (belligerent nexus)"[17].

These criteria do not cover only conventional participation in hostilities like using weaponry by civilians to attack the enemy but also activities like cyber network attack (CNA) or any civilian behaviour in cyberspace operated to "disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computer and networks themselves, which may be conducted over long distances through radio waves or international communication networks"[18].

The threshold of the harm condition is met when there is an objective likelihood of harm as a result of action. This means that there is no necessity for the materialization of harm as such. Cyberspace gives a lot of opportunities which do not directly harm an enemy but could start a chain reaction of many consequences just to mention the possible results of an eventual attack on a power plant, public transportation system, health care system etc. Simply taking this into account a cyber network attack can be as deadly and hazardous as a traditional attack. It can inflict death, injury or destruction on persons or objects protected against a direct attack. Therefore, using a personal computer in order to cause harm for an enemy definitely suits the threshold of the harm requirement.

Direct participation in hostilities via the Internet mostly has a direct causal link between the act (hacking, DoS) and the harm itself. However, in order to qualify each action as one's direct participation in hostilities a civilian must perform it him/herself. The mere facilitating of a general war effort is not enough to meet the direct causa-

17 These three criteria are constitutive elements of direct participation in hostilities developed in *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law* p. 46-64.

18 The definition of CNA remains still inconsistent. However, for the purpose of this article the most suitable is the one from the Background Document DPH 2003 p. 15 ff. with references.

tion criterion. Any harm to the party of the conflict should be brought in one causal step. Moreover, even "where a specific act does not on its own directly cause the required threshold of harm, the requirement of direct causation would still be fulfilled where the acts constitutes an integral part of a concrete and coordinated tactical operation that directly causes such harm"[19].

Thirdly, apart from these two objective requirements any direct participation hostilities shall consist of a third subjective element, precisely an act specifically designed to do so in support of a party to an armed conflict and to the detriment of another (belligerent nexus). Therefore, no conduct lacking a sufficient nexus to the hostilities could qualify as direct participation in hostilities[20]. Civilians cannot directly participate in hostilities if they are totally unaware of the role they are playing in the conduct of hostilities. An example of such a situation in cyberspace is when a hacker unintentionally acting on behalf of the government thinking his task has nothing to do with the conduct of hostilities.

The first conflict which took place in cyberspace is the one in Kosovo[21]. During that conflict Serbian hackers (hacking groups such as Black Hand or Serbian Angel) used a wide range of means in order to stop the bombardment of Belgrade by NATO forces. They used the Internet for propaganda, communication, disinformation of the enemy, virus attacks, DoS, DDoS, e-mail bombing, so called Yugospams etc[22]. Even presuming the presence of the subjective hostile intent of hackers these examples cannot be interpreted as direct participation in hostilities because they lack the necessary threshold of harm (no adverse affect on the military capacity of NATO or infliction of death, injury or destruction on persons or objects protected against direct attack) as well as such mere propaganda can only be understood in terms of an indirect causal link because the eventual harm neither was brought in one causal step nor it was a part of a general Serbian strategy. Internet propaganda was also used by Pakistani hackers in their conflict with India in 1998. They attacked mostly the websites of nuclear concerns such as the Bhabha Atomic Research Center (BARC) or the India Gandhi Center for Atomic Research (IGCAR) as well as governmental websites[23]. They also established online manuals for amateurs in order let them know how to attack Indian websites using mostly DDoS attacks[24]. The even managed to steal some data on the Indian nuclear program[25]. Such

19 Report DPH 2004, p. 5; Report DPH 2005 p. 35 f.

20 Report DPH 2005, p. 25.

21 D. E. Denning, *Activism, Hacktivism, and Cyberterrorism: the Internet As a Tool for Influencing Foreign Policies*, [in:] *Networks and netwars. The Future of Terror, Crime, and Militancy*, ed. J. Arquilla, D. Ronfeldt, Santa Monica 2001, p. 248.

22 Ibidem, p. 240.

23 R. Visvesvaraya Prasad, *Hack the hackers*, "Hidustan Times" 19th December 2000.

24 S. Bhattacharjee, *War in cyberspace*, "The Indian Express" 31st May 2002.

25 S. Sristava, *Indo-Pak war raging in cyberspace*, "The Times of India" 3rd January 2002.

behaviour comparing to that of Serbian hackers reaches the necessary threshold of harm as well as other two requirements. Therefore, it may be described as direct participation in hostilities.

One of the most extensive cyber conflicts took place between Israel and Palestine. Palestinian hackers launched an open campaign against Israel called Electronic Intifada and one of the hackers group called Unity established a four year program of internet war in order to destroy the Israeli's internet infrastructure[26]. Israeli hackers responded with DDoS attacks actively blocking six Hezbollah websites. Cyberspace military actions became one of the priorities for the Israeli army at the beginning of the 21st century[27].

Direct participation in hostilities does not only include the immediate execution phase like hacking, performing DDoS or taking control over the enemy's information system but also preparatory measures taken to execute an act itself as well as the deployment to and return from the location of its execution, where they constitute an integral part of such a specific act or operation[28]. This concerns especially hackers specialized in virus creation. Before launching a virus attack it is necessary to produce them. Such conduct may be seen as a preparatory measure in order to perform a direct attack. However, there are also situations in which the virus is simply bought from a creator and then used by a totally different person or entity. Unless a creator has knowledge about his client's aims he should be held liable as the mere creation of a virus which does not fulfil the threshold of the harm requirement is still a part of the operation as such adversely damaging the opponent. Of course buying computers and items necessary to perform a cyber network attack as well as learning abilities or gathering intelligence to do so can be seen as a preparatory measure but only if it directly aims to perform an attack.

The deployment and return after the execution of a specific act of direct participation through the Internet generally does not include geographic displacement. However, if the perpetrator after committing an attack performs the actions in order to hide his presence in the web or simply eliminate all the traces it shall be seen from this perspective as a form of deployment and return. The same can be said about blocking of eventual pursuit. The direct participation in hostilities therefore begins with the first action taken in order to attack the enemy, it finishes when a civilian stops to attack and separates him/herself from the action.

26 C.J. Gentiler, *Hacker War Rages in Holy Land*, "The Wired" 8th November 2000.
27 Ibidem.
28 Report DPH 2006, p. 54-63.

Loss of protection as a consequence of direct participation in hostilities in cyberspace

Civilians enjoy protection against direct attack unless and for such a time as they take a direct part in hostilities (taking into account preparatory measures and deployment and return after its execution)[29]. In other words their protection is temporarily suspended. What is necessary to mention is the fact that a civilian can regain his/her protection anytime. In order to do so he/she has to stop participating in hostilities. In the case of any doubt, a civilian must be seen as the one not directly participating in hostilities. Every civilian's behaviour must be interpreted in good faith due to the just assessment of the prevailing circumstances. This is a difficult task especially in cyberspace. Taking into the consideration hacking skills which enable camouflage the identity of a civilian may create a long path for attack including a cross-border attack. In order to evaluate each of the examples it is necessary to have also some knowledge and abilities about cyberspace and cyber network attacks. It is extremely hard to establish which from the mouse clicks was the first and started a civilian's direct participation in hostilities. For sure it is not the last "enter" which commences the attack, but also turning the computer on should not be the one in question either.

However, it is almost impossible to attack a civilian who directly participates in hostilities the moment he/she does so. It is caused by the tracking time. Even if we establish that civilian "A" is responsible for the particular attack on the power plant we cannot attack him/her as he has/she already stopped to participate. This however does not mean that he/she cannot be prosecuted for the criminal behaviour against a particular state including perfidy or other activities prohibited by IHL[30]. The difficulty lies here in the fact that very often states do not wish to cooperate in the determination of the path of the attack. That is one of the factors which makes civilians practically unaccountable. Such impunity often encourages others to perform the hacking activity.

Before attacking all feasible precautions must be taken to verify that targeted persons are legitimate military targets[31] and there is no risk of causing incidental loss of civilian life, injury to civilians and damage to civilian objects[32] as well as other incidental harm that would be excessive compared to an anticipated military advantage[33]. Moreover as in the case of a combatant a direct attack against a civilian must be suspended or can-

29 Art. 51 [3] AP I, Art. 13 [3] AP II.

30 *V.* ICTY, Prosecutor v. Tadić, Case no. IT-94-1-AR72, Decision on the Defense Motion for Interlocutory Appeal on Jurisdiction of 2nd October 1995, para. 67, 70; ICTY Prosecutor v. Kunarac et al. , Case no. IT-96-23, Judgment of 12th June 2002 Appeals Chamber, para. 55 ff.; ICTR, Prosecutor v. Rutaganda, Case no. ICTR-96-3, Judgment of 23rd May 2003, para. 569 ff.

31 Art. 57 [2] (a) (i) AP I.

32 Art. 57 [2] (a) (ii) AP I.

33 Art. 57 [2] (a) (iii) AP I and art. 57 [2] (b).

celled if he or she becomes *hors de combat*. The problem lies in the determination of such a situation namely what does *hors de combat* mean in the case of hostilities conducted in cyberspace? Turning the computer off? Also the means and methods of attacking civilians involved in cyber warfare are not unlimited[34]. In other words the use of force against civilians not entitled to protection against direct attack remains subject to legal constraints derived from IHL norms namely the principles of military necessity and humanity. These principles have also a major role in determining the level of the attack on a civilian directly participating in hostilities who does it in his/her private house at the same time taking care of his/her children. For sure launching a rocket to destroy his/her premises along with all the innocent civilians around him/her would be in contradiction with the above mentioned principles. Referring to the famous words of Jean Pictet it can be said that "if we can put a hacker out of action by capturing him, we should not wound him; if we can obtain the same result by wounding him, we must not kill him. If there are two means to achieve the same military advantage (in our case stop a civilian from a cyber network attack), we must choose the one which causes the lesser evil"[35].

Conclusion

In any modern conflict, cyberspace can be an additional avenue of attack. Cyber attacks are not launched frequently by a state itself, but by an individual or group of citizens. It can be under assault from cyber-spies, thieves, saboteurs and hackers. Their goalis to defeat and weaken the enemy party without fighting. Its rapid horizontal escalation is based on three reasons. First, the main criteria for civilian hacker attacks appear to be the vulnerability of targets. Second, international hacker groups like Anonymous view the situation as one in which they can wield power without fear of retaliation. Third, the more bipolar a conflict is, such as those which we have witnessed, the greater the chance that it will attract volunteers to one side or the other[36]. Moreover, civilians willing to directly participate in hostilities do not need to obtain conventional weapons; instead they can simply create and send viruses from their home computers and while performing it they can still remain anonymous or even steal an identity and pretend being someone else. This includes perfidy. The current practice shows however that cyber network attacks very rarely take the form of direct participation in hostilities under IHL mostly because of the lack of a threshold of the harm requirement. However, an Estonian example of taking control over the railway infrastructure represents the

34 Art. 22 H IV R. Art. 35 [I] AP I.

35 *V.* J. Pictet, *Development and Principles of International Humanitarian Law*, Dordrecht 1985, p. 75.

36 *Cf.* P.D. Allen, *The Palestinian-Israeli Cyberwar*, "Military Review" March-April 2003, p. 55.

growing tendency of not only blocking governmental websites based on DoS attacks but also attacking strategic points in order to disrupt the functioning of the state itself.

The future of armed conflicts is definitely connected with cyber attacks mostly from the non-state actor's side. It is used by them in order to balance the difference of power. Here the single man with special abilities can keep in check the whole country as the United States of America. The more the state depends on cyber infrastructure, the more it is vulnerable for the potential attack. The cyber activity of civilians can be interpreted in the terms of direct participation in hostilities, however this is a difficult task. Not all such activities subsequently fulfil the requirements of the threshold of harm, direct causation and belligerent nexus. On the other hand some of them do. Moreover, mouse clicking can be seen as an involvement in hostilities for many reasons like propaganda and disinformation, enhancing the general war effort and often as a particular kind of involvement namely direct participation in hostilities. What will bring the next cyber conflict? I do not know, but for sure, any civilian must be aware that even because of such mouse clicking aimed at causing an enemy harm he or she is deprived for such a moment from the protection of the international humanitarian law of armed conflicts.

Summary

Can mouse clicking be seen as involvement in armed conflict? Some notes on the direct participation in hostilities in cyberspace

Contemporary armed conflicts are increasingly based on new technologies. These technologies enable to conduct hostilities from a distance, often eliminate the human factor from the battlefield. Nowadays, cyberspace created by the Internet allows to frame the idea of armed conflict outside the traditional recognition of the fight between belligerent armed forces. This article addresses issues of the direct participation of hostilities in cyberspace. In the first part it discusses technological development and its impact on the activation of the civil factor during armed conflicts. In the second part by analysing the current practice of cyber conflicts it refers to the concept of direct participation in hostilities and its constituent elements as a threshold of harm, direct causation, belligerent nexus at the cybernetic level. The third and final part examines the possibility of the loss of protection, in particular, it addresses the issues related to its temporal nature and the question of means and methods of attacking civilians involved in cyber warfare.

Keywords: Humanitarian law, armed conflicts, cyberspace