Beyond the Battlefield: Navigating the Legal Challenges of Civilian Cyber Participation in Modern Warfare

Ahmed Aubais Al fatlawi

University of Kufa, Faculty of Law *Lecture at Al Alamein institute for Postgraduate studies*

Email: ahmeda.alfatlawi@uokufa.edu.iq

Abstract: The evolution of cyber warfare has muddled the distinction between civilians and combatants, presenting a profound challenge to international humanitarian law (IHL). As conflicts spill over into the digital domain, involving civilians in cyber operations raises complex legal issues. Unlike in conventional warfare, where delineating combatants from non-combatants is more explicit, the complexities of cyberspace pose unique challenges for existing IHL frameworks. This article delves into these emerging challenges, highlighting the legal ramifications of civilian cyberattack involvement and emphasizing the critical need for creative legal solutions. The proliferation of anonymous, decentralized cyber operations undermines the application of the principle of distinction, complicating efforts to safeguard non-combatants and ensure accountability. To address these challenges, the article advocates for establishing new legal standards, including a revised concept of direct cyber engagement that elucidates the roles of civilians and combatants in the digital battlefield. Furthermore, it emphasizes the imperative of setting up specialized international courts or bodies to adjudicate cyber-related cases, essential for ensuring accountability in cyberattacks. The article also underscores the crucial role of enhanced international cooperation in this process. Specialized legal frameworks and international cooperation are vital for upholding the humanitarian principles integral to IHL while adapting to the evolving nature of modern warfare. In conclusion, the increase in civilian participation in cyberattacks uncovers a crucial gap in current legal protections, demanding swift and decisive action to maintain the principles of humanitarian law in the digital age.

Keywords: Cyber warfare; Legal Challenges; Civilian Involvement.

INTRODUCTION

The traditional boundaries separating civilians from combatants have blurred as armed conflicts expand to the digital sphere. The participation of civilians in modern cyber warfare poses unprecedented legal challenges, necessitating a proactive and immediate reassessment of existing legal frameworks. Unlike traditional conflicts, where the lines between civilians and non-combatants are more apparent, cyberspace presents complexities that IHL struggles to address. This article explores these challenges, delves into the legal implications of civilian involvement in cyber operations, and stresses the need to adapt our legal understanding to protect non-combatants while maintaining accountability in this evolving theatre of war.

THE PROBLEM OF THE STUDY

The direct participation of civilians in cyber hostilities poses several significant challenges:

1. Overlapping roles: IHL traditionally distinguishes between civilians and combatants. However, civilians' participation in hostile cyber operations weakens these lines, making it difficult to determine who is a legitimate target and who is protected under international humanitarian law.

2. Legal ambiguity: The legal frameworks governing cyber warfare are still under development. There are no clear definitions or rules regarding what constitutes direct participation in cyber hostilities, leaving room for interpretation and potential exploitation.

3. Accountability and attribution: Cyber operations often allow anonymity and the use of agents, complicating the attribution of acts to specific individuals or groups. This makes it challenging to hold civilians accountable under existing legal frameworks and to determine when they have exceeded the threshold for direct participation in hostilities.

4. Risk of increased civilian harm: Civilians involved in cyber operations may inadvertently contribute to harm to other civilians or critical infrastructure. Cyber means can have far-reaching and unintended consequences, such as disrupting essential services or causing collateral damage that disproportionately affects the civilian population.

THE IMPORTANCE OF THE STUDY

Writing on the topic of civilian participation in modern cyber warfare is critical for several reasons. As the lines between the roles of civilians and combatants blur in the digital age, there is an urgent need to reassess and refine the legal frameworks governing warfare. Addressing these issues is key to ensuring that IHL remains relevant and effective in protecting civilians, even as conflicts evolve. These writings contribute to a broader understanding of how to strike a balance by exploring legal challenges and proposing solutions. between the protection of non-combatants and the exigencies of modern warfare, ultimately helping to shape future legal standards and policies in this increasingly critical area.

SECTION I: CONSTANT AND VARIABLE IN THE CONCEPT OF CIVILIAN AND DIRECT PARTICIPATION IN HOSTILITIES

By reviewing customary rules codified under international humanitarian law, we have found no indication of a prohibition on the direct participation of civilians in hostilities in general or those of cyber attacks that amount to hostilities. If they participate, the legal situation will change, they will lose their protection and be targeted all the time they assume this role, whether the armed conflict is international or non-international.

In this part of the study, we will try to investigate the concept of civil vis-à-vis other corresponding concepts, including the concept of combatant as well as the concept of direct participation, by discussing the following points:

FIRST: THE CONCEPT OF THE CIVILIAN VERSUS THE CONCEPT OF THE FIGHTER

Before we address the concept of civilian, the concept of combatant must be explained within the framework of international humanitarian law. So, who is a combatant ?

In light of the provisions of international humanitarian law, combatants are: "persons who are entitled by the rules of international humanitarian law to conduct hostilities, and therefore hostile operations may be directed against them; in return, this legal status provides for a permit to target them for killing, wounding or capture, by the restrictions established by the law governing hostilities ".

By analyzing Article 43, paragraph 2, of Additional Protocol I of 1977, which states: "Members of the armed forces of a Party to a conflict (other than medical personnel and chaplains covered by Article 33 of the Third Convention) are combatants, that is to say, they have the right to participate directly in hostilities" , meaning that they have the right to take a direct part in hostilities .

Based on Article 43 (1) of Additional Protocol I of 1977, which states: "The armed forces of a Party to a conflict consist of all organized armed forces, groups and units which are under a command responsible to that Party for the conduct of its subordinates, even if that Party is represented by a government or an authority not recognized by an adverse Party", this definition of armed forces covers, in essence, all persons who fight on behalf of and under the command of a Party to a conflict. The conditions imposed on armed forces also apply to armed groups, and members of such armed forces are, therefore, vulnerable to armed attacks.

This broad functional concept appears more comprehensive than the Hague Regulations concerning the Laws and Customs of War on Land of 1907 and the Third Geneva Convention of 1949 .

(1) Have responsible leadership.
(2) Have a badge that distinguishes it remotely.
(3) Bear arms openly.
(4) Comply in their hostile operations with the laws and customs of war conduct.

These requirements are strictly speaking required of members of armed groups, whenever they are in addition to the regular armed forces, in order to enjoy the privileges of combatants and prisoner of war status after being captured by the enemy .

The concept of affiliation, mentioned in the ICRC's Interpretive guidance, requires proof of the (de facto) relationship between an organized group and a party to the conflict and does not need to be formally declared the relationship, as the relationship can be established through a de facto agreement or conclusive conduct that makes it clear which party the group is fighting for . For example, a state may resort to a group of

individuals to conduct cyber operations during an armed conflict because the group possesses the necessary knowledge or experience that state organs do not. Its members have combatant status as long as it meets other combat requirements. It is important to note that the claim to combatant status can be significantly weakened in fragile groups, particularly online, and members of such a group may have difficulty demonstrating that they are working for responsible leadership, most problematic being that the group undergoes an internal disciplinary system capable of enforcing rules of compliance with international humanitarian law.

Some criticize the ICRC's approach, particularly in stating the concept of civilian participation; in other words, while opinions on the interpretative guidance vary, there is a common concern about its perceived bias towards humanitarian considerations rather than military necessity. This criticism presents a significant challenge, as the law of armed conflict relies on a delicate balance between these two principles. Any inclination towards one over the other disrupts the fundamental basis of the rules of the law of armed conflict. The view that the Interpretative guidance gives excessive priority to humanitarian concerns raises the risk of impractical restrictions on military operations, which may jeopardize a State's military success or survival in conflict.

A fundamental question may arise: What is the attitude towards the advantage (military uniform and the distinctive mark of combatants) in international humanitarian law and the cyber context?

It can be said that another characteristic that must be available is the commitment of armed groups to a specific feature of their own, such as wearing a uniform or placing a distinctive sign, and this has a definite legal significance, which affects armed groups as well as regular armies, which is the distinction of fighters for themselves from others, namely civilians.

This is what is referred to in Article 44 of Additional Protocol I of 1977 and the generally accepted practice of States regarding the wearing of military uniforms to identify combatants of a party to regular units, a goal sought by the article to distinguish between combatants in guerrilla wars, as referred to in Article 48 of the same Protocol in the text: To ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives ".

The ability to distinguish combatants as such is crucial, especially for enemy forces, whether for military purposes or to protect and avoid civilian casualties. Since there is no binding provision in international humanitarian law on warring parties informing each other in uniform, armies must inform each other of distinctive signs and uniforms so that members of hostile forces can be identified as combatants.

Now that we have clarified the fighter concept, we must ask who a civilian is. Can we find a difference in description between those who participate and play a role in an attack with kinetic energy weapons such as machine guns and those who participate in a cyber attack?

According to customary international law, Article 50 of Additional Protocol I defines civilians in terms that reflect a negative functional aspect, i.e. persons who are not members of the armed forces or militias and volunteer units, as well as civilians who do not participate in the popular uprising of defence.

A distinction must be made between civilians and combatants in times of armed conflict based on the principle of distinction. the shift of hostilities from the physical (kinetic) world to cyberspace does not affect the definition of combatants or the negative definition of civilians. However, the changing nature of hostilities to cyber attacks may make the distinction between battlefields and civilian character less clear, as an increasing number of civilians can be directly involved in hostilities in various ways, unaware of the consequences of their actions.

Cyber means have provided a number of new possibilities for non-combatants who wish to participate in hostilities. Access to cyberspace is not limited to advanced armies but to non-state actors, armed groups, and individuals, who can directly participate in cyber hostilities from almost anywhere.

The development of digital technologies and the ease of widespread access to cheap "hacker tools" have allowed non-state actors to obtain several security loopholes for militaries that rely on digital communications.

On the other hand, the difficulty of revealing the identity and nature of cyberspace boundaries

has motivated many (hostile) parties to exploit these security vulnerabilities, making hostile cyber attacks an attractive way of armed violence from a distance, with all its accompanying legal challenges.

A review of contemporary armed conflicts will reveal that civilians are highly present and active on the battlefield, and this can be summarized in two roles in particular: first, as mercenaries or members of private security and military companies to carry out offensive and defensive cyber hostile operations, and second, as pirates (civilians) who make similar contributions. In response to this increased civic engagement, the ICRC decided to establish a project on the idea of direct participation in hostilities, the outcome of which was the publication of the ICRC Interpretive Guidance in 2009.

The project is designed to answer three questions:

First: Who is considered a civilian for the principle of discrimination?

Second: what conduct amounts to direct participation in hostilities?

Third: What conditions determine the loss of protection from targeting?

The above draft and the resulting interpretative guidance did not seek to change customary or treaty IHL but rather reflected the ICRC's position on interpreting existing IHL in light of the circumstances prevailing in contemporary armed conflicts. It is a non-binding document for States, even if it could affect State practice.

Although the targeting regime proposed in the Interpretive guidance only expresses the views of the International Committee of the Red Cross, which were later criticized, it represents a valuable and essential step to understanding the idea of direct participation in hostilities, as the Interpretive guidance lines are the most comprehensive work on this subject so far. The general principle of direct participation in hostilities prevails.

Because the topic of direct participation of civilians in the context of cyber attacks in the light of the interpretive guidance has been focused, the study will partially follow the outline of these guidance lines by analyzing the relevant points, namely the foundational elements of the concept of direct participation and its time scale governing the loss of protection, precautions and assumptions in case of doubt, as well as a comparison between the application of the Tallinn Manual of the concept of hostile participation with the ICRC Interpretative guidance.

To align the research framework with the above, we will try to research the second part of this section to examine the constituent elements of direct participation.

SECOND: THE CONSTITUENT ELEMENTS OF THE CONCEPT OF DIRECT PARTICIPATION IN HOSTILITIES

Several professors point out that the increasing participation of civilians in armed conflicts is a worrying trend that requires our attention. Whether civilians are victims or participants in hostilities, they play a more prevalent role on today's battlefield. This transformation, often called the civilianization of armed conflict, is a direct result of more extensive operational changes, including the outsourcing of combat functions to private entities, the use of civilian agents by States. and the spread of advanced war technology. It is essential that we deal with this trend and understand its implications to ensure that the lives of civilians in conflict areas are protected.

Reviewing the Interpretative guidance, we find the fifth recommendation, "Elements constituting the concept of direct participation in hostilities", which is the essence of interpretive guidance.

To count a civilian as a direct participant in hostilities, three cumulative criteria are required: first, a certain threshold of damage must be met (damage threshold); second, there must be a direct causal link between the act in question and direct damage (direct causation), and third, the act must be designed to support one of the parties to the conflict and harm the other party to the conflict (the relationship to the war act).

It should be noted that although "several experts expressed specific concerns about certain aspects of the constituent elements, most considered them to reflect a broad understanding of the group." They can be summarized as follows:

1. Damage Threshold

The first cumulative criterion is called the threshold of damage. It requires the possibility

that "an act by a civilian would adversely affect the military operations or capability of a party to an armed conflict or, in any other way, cause death, injury or destruction to protected persons or objects protected from attack directly".

The effects of hostile behaviour "should most likely" lead to, but not necessarily have resulted in the desired result. In other words, the damage threshold can be reached without or before the damage materializes; the risk of damage is sufficient, requiring that the damage take material form, but only an objective probability that the act will result in such damage in the prevailing circumstances.

On the other hand, military damage must be interpreted in the narrowest scope, i.e. not only death or injury to combatants or destruction or disruption of military objectives but also any consequences that would adversely affect the hostilities or military capability of a party to the conflict.

Examples include sabotage or unarmed activities that restrict or impede the deployment of forces or communications or facilitate the arrest or seizure of military equipment by military members. Electronic jamming operations, whether through cyber attacks, wiretapping the telephone calls of the adversary's high command, or transmitting information about the tactical targeting of the attack, may suffice." It should be emphasized that the damage threshold is higher and within a military scope.

The Interpretive guidance excluded from the application of direct participation in hostilities acts by a civilian that leads to "interruptions of electricity, water or food supplies or manipulation of computer networks." Isn't such exclusion illogical, as such actions could seriously affect public security, health and the economy?

The existence of significant adverse military effects (type and degree of damage) is required to say that there is direct participation in hostilities. Still, the decisive criterion is the impact of such attacks on enemy military operations.

that the foregoing is consistent with the requirements contained in Article 52, paragraph 2 of Additional Protocol I: "Attacks shall be limited to military objectives only, and military objectives shall be limited in respect of objects to those which make an effective contribution to military action, whether by nature, location, purpose or use, and whose total or partial destruction, capture or deactivation in the circumstances prevailing at the time would provide a definite military advantage", In other words, those identified as "military objectives". Conversely, targeting objects that do not contribute militarily or give the adversary a military advantage would not qualify for direct participation, and therefore, if the cyber attack does not rise to the level of negative military effects, in accordance with Article 52(2), we will not be here to participate actively and directly in hostilities. The explanatory manual seems to refuse to count any cyber attack as a direct participant, except for what was directed at an enemy military force and caused material damage similar to that resulting from kinetic means and methods of warfare.

By drawing an approach between the Interpretative Guidance and the Tallinn Manual concerning the threshold of harm, we find a clear difference between them. While interpretative guidance requires that harm be embodied in fact or that there is a reasonable probability that it will be achieved as an "objective probability", the Tallinn Manual uses the term "intended or actual effect". In other words, the harm threshold would mean being met if a civilian had the "intent" or "intent" to cause harm and could be objectively identified.

A civilian who intends to cause sufficient harm and carries out a hostile cyber attack with no opportunity to influence the adversary will lose protection as a civilian and even more, as he will be seen as a direct participant in hostilities under the Tallinn Manual. All of this will lead to a minimum level of protection for civilians participating in cyber hostilities, making them easier to target.

2 .Direct causation

The second cumulative criterion is called "direct causation" and requires a direct causal link between hostile behaviour and potential harm, either by that behaviour or by a coordinated military operation, of which such behaviour is an integral part.".

From the foregoing, direct causation means that the harm in question must occur in a "single causal step." To meet the criterion of direct causation, a particular act must directly cause or be expected to cause damage that meets the first criterion (threshold of damage) alone or as an integral part of a cumulative process.

A causal relationship in cyber attacks can be achieved even if the malicious behavior has been committed beyond the scope of the battle. for example, a civilian who develops or develops hostile cyber software; based on this example, the Interpretative guidance provided evidence clarifying the requirement of direct causation and promised to assemble and store an "improvised explosive device, (even if the assembly and storage of this improvised device) may be related to the damage caused by a series of uninterrupted events, but it does not cause that damage directly, unlike implanting and detonating that device. In most cases, cyber means must be designed for a specific cyber attack. In other words, there appears to be a direct causal relationship between the production and development of cyber means and the expected harm, so their producer or developer can be considered a direct participant in hostilities .

In a related context, many problems have been raised about causation and topics unrelated to cyberattacks, such as using drones. The exciting issue was adapting behavior and linking it to harm as a condition for direct participation. In other words, who is directly involved? Did the one who launched the plane, its face and its walk-in weather? Or does the issue go beyond the battlefield to those who ordered, planned, arranged, and prepared for the use of drones?

Several specialists have pointed out that the subject is subject to extensive research and discussion, especially in linking direct participation with another topic, which is direct responsibility, as they focus on issues compared to the jurisprudence of international criminal courts and in selected cases, especially the original direct contribution, which arises whenever the accused is responsible for the material act of the crime (actus reus).), in other words, who was on the actual field, as we find in the jurisprudence of the International Criminal Tribunal for the Former Yugoslavia in the case of The Prosecutor v. Fatmir Limaj .

The Court held that direct responsibility for any crime committed was first directed against the person who carried out the material disposition of the crime, whether by act or omission .

By analogy, cyber attacks cannot be attributed to existence as an object, except through programs managed through devices, which are a means subject to the command of a person and remotely. This behavior means that there is a link between the offensive operations carried out by these programs, resulting in violations against international humanitarian law, and those who activated them to make the immediate decision to identify and address the target.

Following the foregoing, direct responsibility requires compelling evidence that those who used cyber software were aware and predicted that the circumstances surrounding the attack would undoubtedly encounter serious violations, yet continued to use and direct in a manner that suggested a determination to accept the consequences of the attack. It is more complicated if cyber software is the one that takes the identification and processing of targets after it has been activated.

In this case, the user is directly responsible, whether he or she is in control of the software decisions themself or has activated self-decision software.

The above order was referred to by several researchers regarding the approach to crimes committed by cyber software, by analogy with the legal situation and in cases heard by international criminal tribunals, such as the Rwanda Tribunal in the case of the Prosecutor v. Mahimana, in particular in paragraph (479) of its judgment, as both Ezio Di Nucci and Filippo Santoni de Sio refer to) that in the Mahimana case, the Court took the narrow direction of determining criminal responsibility by emphasizing the following: "Advance planning is sufficient evidence that the offender Egypt to carry out the conduct constituting the crime following its intentional or probabilistic context, and that the criminal intent of this type of responsibility is confirmed in planning as a first step towards execution or with a high probability of complacency that a crime will be committed in the course of an act ".

By analogy, cyber software's production, development, or development does not negate the causal link between conduct and harm if reasonable grounds suggest that it can be used in any hostile operation. In other words, the threshold of harm is achieved when a cyber company official is aware that such programs can easily reach civilians, leading to a direct contribution to hostilities, and they accept this possibility.

In light of this criterion, the collective and complex nature of contemporary military operations must be considered, as the

Interpretative guidance gives an example of persons involved in an attack carried out by a drone. The direct causal relationship includes acts that do not cause harm except in conjunction with other acts. In other words, a condition may be fulfilled if the action is an integral part of a concrete and coordinated tactical operation that directly causes that damage, and then in the case of a mass cyber attack, even if it is a contribution, A civilian cannot satisfy causation on its own, so a civilian can be considered a direct participant in hostilities because of his active involvement in that process. Intentional and (unintentional) damage is likely to occur through several causal steps, for example, via Stuxnet software, which may cause damage through several coordinated actions (hacking, exploitation, modification) as parts of a concrete tactical process.

It remains unclear whether cyber attacks can meet the requirements of direct causation, which, in the opinion of some specialists, means that civilians can participate in direct cyber hostilities with impunity.

Finally, we conclude that the condition of direct causation refers to a certain degree of proximity of cause to damage. This element should not be confused with only two other semantic elements, namely - temporal proximity and geographical proximity to the hostile action - that is, even if the hostile act is committed through remote control means, such as a drone or through cyber attacks, since the person committing the act, geographically distances himself from the damage caused, or from During a delayed operation, i.e. time-distant mechanism, such as a timer-controlled explosive device, in this case, the causal relationship between the use of such means and the damage caused by them remains direct, regardless of their temporal or geographical proximity.

Contrary to the above, the persons who feed the armed forces are close in time and geography to hostilities. Still, the relationship between their support and the maximum damage required against the enemy remains indirect in hostilities. Thus, while the temporal or geographical proximity of damage resulting from a specific act indicates that the act amounts to direct participation in hostilities, those factors will not be sufficient in the absence of a direct causal link. The element of direct causation must be determined based on the harm that could reasonably be foreseen to occur as a direct result of a concrete action or action.

3. Relationship to war action

The third and final cumulative criterion (relation to the act of war), which is the least controversial of the above, is that to satisfy the requirement of association with the act of war, the action must be specifically designed to directly cause the minimum required for damage, in support of one party to the conflict at the expense of another.

In general, the harm resulting from self-defence against acts of violence prohibited under international humanitarian law, under control and exercise of authority over persons or territory, as part of civil unrest against that authority or during acts of violence between civilians lacks the element of relevance to the act of war required in classifying the act as direct participation in hostilities.

On the other hand, hostile cyberattacks do not change or specifically affect this criterion, as the relationship between a war act and opportunistic criminal activities in cyberspace must be distinguished. This criterion must be analyzed with great care. Direct participation in hostilities and criminal activities can be closely linked.

In general, the criterion of relation to the act of war and acts constituting a crime of a personal nature that occur during an armed conflict excludes the criminal, as a criminal who uses cyber means to steal the funds of a party to the conflict with the aim of achieving private gain will not be a direct participant in hostilities.

In a related context, the Interpretive guidance distinguishes between the concept of relation to a war act, which depends on the objective purpose of the action and does not depend on the subjective intent of each individual involved, and hostile intent, which relates to the state of mind of the person concerned. However, the Interpretative guidance identifies exceptional cases of persons unaware of their role in the conduct of hostilities. For example, a driver unaware that he is transporting a bomb in his wheel, which is controlled remotely), in this case such a civilian in such exceptional circumstances cannot be counted as performing a hostile act in the sense of the phrase and thus remains protected from direct attacks, even though the military operation in which he was exploited is linked to hostilities. As a result, the situation of this civilian and the situational contexts must be taken into account when assessing proportionality during any military operation likely to cause incidental harm.

Some scholars have called for a reconsideration of existing international regulations to address the challenges posed by cyberattacks, particularly concerning the involvement of civilians. There is an emphasis on the potential need for explicit legal provisions that recognize actions such as forcing an electrical grid or power plant out of service, or disabling access to essential government websites and online systems (including those run by consulates and embassies) as constituting acts of violence against the civilian population, particularly when such actions could lead to severe consequences like the inability to access vital services for days or weeks. In such cases, it would be difficult to argue that the primary objective was not to spread terror among civilians.

The advanced approach may be challenging to achieve, especially in proposing the adoption of a new convention regulating the use of cyberattacks, but this does not prevent us from thinking about revising the two Additional Protocols of 1977, for example, and this will not be expected unless aggressive cyberattacks become so widespread that they are not likely to be outside the framework of international regulation, as is the case with many weapons that were previously outside the scope of international agreement.

Section II :Time range of direct participation in hostilities and suspicion

This section of the study delves into the critical issue of civilian protection during direct participation in hostilities, particularly in cyber warfare. It is divided into two key parts: the scope of the loss of civil protection, including preparatory measures, the spread and return of hostilities, and the duration governing this loss; and the assumptions made in cases of doubt, focusing on the required precautions and the presumption of civilian protection. Understanding these aspects is vital for balancing the protection of civilians with the realities of modern conflict, especially in the evolving cyber domain.

First: The Scope of Loss of Civil Protection

Civilians lose the right to protection from direct attacks during the time range in each specific act that amounts to direct participation in hostilities. and the time range can be divided into two aspects: the first within the limits of direct participation in hostilities (beginning and end), and the second has to do with the period governing the loss of protection, and for the sake of research, we will divide this section into two parts as follows:

1. Preparatory measures

The sixth recommendation of the Interpretative guidance referred to "the beginning and end of direct participation in hostilities," as well as deployment to and from the place of implementation, which forms an integral part of hostilities," with a discussion of preparatory measures.

According to the interpretive guidance, a distinction must be made between preparatory measures aimed at carrying out a specific hostile act and preparatory measures aimed at establishing the general capacity to carry out unspecified hostile acts, as only the first constitutes an act of direct participation without the second, which confirms the element of direct causation as discussed before, as each cyber means needs to be designed for a specific purpose. Therefore, in most cases, preparing cyber means (production or development) will constitute an act of direct participation. It is also important to note the temporal and geographical proximity of the preparatory action before carrying out a specific hostile action, as it is not necessary for the preparatory action to be classified as direct participation in hostilities. In other words, contemporaneity (space and time) is crucial in adapting the cyber medium as part of any preparatory measure.

2. Spread and return

On the issue of proliferation and return from a specific hostile act, the Interpretative guidance specifically mentions cyber attacks by saying: "When the execution of a hostile act does not require geographic transmission, as in the case of computer network attacks or the case of remotely guided weapons systems, then the duration of direct participation in hostilities is limited to the immediate execution of the action and to the preparatory procedures that form an integral part of such action."

The Tallinn Manual, on the other hand, takes the opposite position: Since the Interpretative Guidance states that Any act of direct participation in hostilities makes a civilian a target for the duration of the period in which he or she takes a direct part in such action, all Tallinn experts agree that actions preceding or following a hostile action are considered to be

within the period of direct participation in that action. According to some experts, they have reduced it to the phrase "upstream to downstream as a causal link", for example, navigation to and from the computer's location used to launch attacks. A cyber attack may begin as soon as an individual starts scanning the enemy's target electronic system, looking for weaknesses, and extends for the duration of hostile activities against that system, and also includes the period during which the damage is assessed to determine whether repeated attack is required.

Also necessary in the cyber context (delayed effects), for example, the placement of a digital loophole in an enemy target system, designed to activate in time of need (receiver); in this matter, the majority of ISAR members took the position that: "The period of direct participation of an individual extends from the beginning of his or her participation in the planning of hostilities to the moment he or she ends an active hostile role in the operation."

In the above example, the period of direct participation will extend from the start of planning to the period of activating the digital baffle through activation, based on an order from the controller, control and operator, noting that the end of the direct participation period may not necessarily correspond to the point where the damage occurs, as one person can work to enter the digital divide, while another person activates it later, the important basic rule is related to the possibility of targeting, that is, making sure that the participation of a particular individual begins and ends.

3. Duration governing loss of protection

In reviewing the Interpretative guidance, we find that the section devoted to discussing this issue is one of the most controversial: according to the Additional Protocols of 1977, a civilian loses his right to protection as such, throughout the time he or she is directly participating in hostilities. Although this wording was highly controversial during the Protocols, it reflects a rule of customary international humanitarian law.

The loss of protection for any specific act of a civilian that reaches the threshold of direct participation in hostilities and its restoration between each act is generally called a "revolving door" ,a term that first appeared in Colonel W. W. Hayes' titled "Air Warfare and the Law of War" in 1990, and is still used by the International Committee of the Red Cross (ICRC) when referring to the participation of civilians in direct hostilities.

The term revolving door refers to the continued loss and restoration of protection from attack during hostilities, and it is essentially defined by periods of engagement for civilians. How long this conceptual door remains open depends on the duration of direct participation. In other words, civilians are protected from attack when the "door" is open and become targeted when it is closed.

The Interpretative guidance has stated its position on this issue, based on it: each action must be treated separately in terms of analysis (participation and result), during which the civilian is restored to protection between each act, in other words, the right to protection of civilians directly participating in hostilities is temporarily suspended, for the duration of their participation in hostilities, and that right is restored after the cessation of involvement.

The Interpretative guidance's view on the "revolving door" is essential for the protection of civilians, an integral part of international humanitarian law, and cannot be considered a legal loophole. The purpose of the idea of direct participation in hostilities is not to punish a civilian who is directly participating as prohibited behavior but as a result of voluntary conduct that may arise in the conduct of hostilities.

The opinion of the experts in the Tallinn manual on this issue was divided, and some of them considered that if the revolving door is possible in kinetic means, it is not so in the cyber context, as the ability to target a civilian who launches repeated cyber attacks starts from the first step within a cyber attack and continues throughout the duration of the activity, albeit intermittently.

In light of the revolving door, the issue of applying or deactivating protection rules in the cyber context is complex to apply to participating civilians. The difficulty can be summarized with the phrase (launching and detecting the attack): the first is related to the speed of launching cyber attacks, and therefore, it seems that the direct participation of civilians is challenging to deal with due to the short period of time, while the second is that most cyber attacks are not discovered until after they have occurred, and at that time the (civilian) perpetrator may have returned to his civil status and has already regained protection.

By reviewing some national practices on cyber civilian engagement, Germany agrees with the view, for example, that "cyber interference in military computer networks [...], whether through attacks on or exploitation of computer networks, as well as wiretapping at the adversary's high command or tactical transmission," as well as "targeting information for attack," could be sufficient to consider a civilian as a direct participant in hostilities.

It is true that the most critical challenges that will face the rules of attribution at the international level, as well as those related to the triggering of international responsibility, are embodied in what can be called the grey zone; in other words, the difficulty of determining the time of participation by a civilian in the framework of a cyber attack and then attributing it to the State benefiting from that attack, which will cast a shadow on many failures in the compliance of States, regarding the application of the rules of international responsibility, as well as the rules for the protection of civilians, which we will discuss. in the next section of this study.

Second: Assumptions in case of doubt and precautions required

According to Article 50, paragraph 1, of Additional Protocol I of 1977, "If doubt arises as to whether a person is a civilian or a non-civilian, that person shall be considered civilian." The explanatory evidence expands this assumption to whether or not he (civilian) plays a direct role in hostilities.

Armed forces subjected to hostilities have difficulty complying with the principle of distinction between combatants and civilians participating spontaneously, sporadically or irregularly in a hostile operation. If there is (doubt) as to whether that person has taken a direct part in hostilities, that person is considered a civilian. All feasible precautions must be taken to avoid mistargeting civilians who are protected from attack.

But what precautions should be taken, and what estimates should be made in case of suspicion related to cyber participation? This is what we will try to look at as follows:

1. Possible precautions requirement

Possible precautions were mentioned implicitly and for the first time in Article 22 of the Hague Convention of 1907, and then clearly and clearly codified in Additional Protocol I of 1977 to the Geneva Convention of 1949 in Article 57 thereof, as well as as as a definition in the Convention on Conventional Weapons of 1980., the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects in Protocol III, on Prohibitions or Restrictions on the Use of Incendiary Weapons, is defined in Article I, paragraph 3, as defined " feasible precautions with: "precautions that are feasible or feasible in all circumstances at the time, including humanitarian and military considerations."

At the jurisprudential level, Frederick de Molinen defined feasible precautions as: "precautions that are practically feasible taking into account the tactical situation, that is, all the conditions existing at a given time, including humanitarian and military considerations."

Niels Melzer defined it as "practical or feasible precautions taking into account all the circumstances prevailing at the time, including humanitarian and military considerations, and in addition, any attack against a civilian who has become hors de combat must be cancelled or suspended".

The International Criminal Tribunal for the Former Yugoslavia (ICTY) and the Kupreškić case have affirmed that precautions in attack are a customary requirement, as it sets out and embodies a pre-existing general rule.

In a cyber context, it may be more difficult without it than in kinetic contexts, as the possible precautions may be limited in scope, given the speed at which cyberattacks are conducted. However, this will not exempt those responsible for any cyberattacks contrary to what the precautions require. For example, in the Galic case, by analogy, the ICTY held that logic dictated that a person was well informed is reasonable in the same circumstances as the actual attacker and also makes reasonable use of the information available to him, and whether he can expect in such circumstances that the attack will cause excessive civilian death and injury.

The criterion of objectivity means that the leader or planner of the attack must behave as a rational and wise person in such circumstances. So Kalshoven argues that the objective criterion is that the usual attacker is well-informed and uses reasonably available information.

To promote compliance with the principle of feasible precautions in international law and to

exercise the right of legitimate defence vis-à-vis the crime of aggression, we recall that States and their armed forces must also take all feasible precautions to minimize harm to civilians, civilian objects and sovereign interests. This duty is objective and evidentiary, represents the substantive duty of the law in question, and constitutes an essential element of proof.

Objectively, both the law of the right of war and the law of countermeasures gradually recognize that due diligence is an element of proportionality, at least in the interconnected cyber domain. Reflecting this emerging duty, when a State engages in legal self-defence against another State, the unintended effects on third State networks arising from self-defence would constitute an unlawful use of force. On the other hand, possible precautions that would reduce this proliferation are a reasonable guarantee of the prohibition on the use of force imposed by the law of grounds of war. Similarly, networks' "interconnected nature" makes due diligence an element of proportionality in countermeasures.

2. Presumption of protection of civilians

In case of doubt as to the conduct of a civilian in the context of collective participation in hostilities, it must be assumed that the general rule for the protection of civilians applies in the first place; in other words, that the conduct of a civilian has nothing to do with hostilities.

On the other hand, the standard of uncertainty applicable to targeting decisions cannot be compared with the strict standard of suspicion applied in criminal prosecution. It must reflect the level of certainty reasonably attainable in the circumstances prevailing in each case. To determine precisely, it is necessary to consider, among other things, the intelligence available to the decision-maker, the urgency of the situation, and the damage that the wrong decision is likely to cause against people protected from direct attacks.

In the Tallinn Manual on the question of the applicability of the presumption (non-direct participation), the Group of Experts was divided into two parts: in the event of doubt as to whether a civilian was directly involved in hostilities, no participation was assumed, and the opposing position of the experts was that in case of doubt, the attacker must, as a legal requirement, review all relevant information and act reasonably in the circumstances prevailing when deciding to target.

Although IHL was initially created to regulate hostilities in the physical world involving violence accompanied by kinetic energy, it also applies to cyberattacks in digital space, especially in light of their increasing use for hostile purposes.

By analogy with kinetic attacks, it is recognized that IHL applies only when a cyber attack is reasonably expected to cause injury or death to people or damage or destroy objects.

What is controversial is the question: What is the position on deleting digital data belonging to the enemy? Does it also constitute damage and destruction, and can the data constitute a military objective? To answer, we say that the use of the same criteria in a kinetic offensive operation and comparing them to assess whether a particular cyber operation also constitutes an attack to which the rules of distinction, proportionality and precautions in the full conduct of hostilities apply, requires careful consideration, especially in several issues, including The boundaries of what is considered permissible for targeting are limited only to what meets the definite military advantage, in other words, it is not possible to authorize the targeting of the infrastructure of a humanitarian nature, such as the deletion of military hospital data, As a reason to affect the morale of combatants, yes, a large-scale cyber attack may be accompanied by the disruption or destruction of military and other data protected in accordance with international humanitarian law. In this regard, prior and reasonable expectations from an experienced person are reliable in determining direct participation.

Marco Sassoli and Lindsey Cameron argue that an experienced military commander, due to their understanding of the interdependence of infrastructure, can foresee the consequences of destroying an electricity utility (such as cutting off potable water to civilians). At the same time, a reasonable average person might not be expected to make this association, which is the preferred criterion, because it excludes negligent behavior that does not meet the objective degree of expectation we support.

Although experts have tried in the Tallinn Manual to apply current international humanitarian law and other rules of international law to cyberspace and cyberattacks, the concepts of direct participation in hostilities and treachery

and the concepts of military targets and attacks do not fit reasonably with the technical realities of cyberspace, as the relevant and dual-use nature of cyberspace makes the application of the principle of distinction more difficult, but not impossible.

The biggest challenge facing the world is in the widespread cyber targeting against infrastructure, especially health ones, in a statement by Ms. Véronique Christory (Senior Arms Control Advisor at the ICRC), in a statement she delivered to the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security on September 10, 2019. She stressed that the healthcare sector may be vulnerable to cyber attacks, like other sectors that represent the infrastructure of critical facilities in any country.

In the first chapter, we have pointed out that the crime of cyber aggression will be the broadest and most challenging to comply with the rules of international law, in particular, the right to self-defence. In this part of the study, we emphasize that the scariest is yet to come, as highly autonomous proactive cyber capability, although still somewhat rare in practice, poses challenges to legal analysis because it does not lend itself to simple measurements and requires careful consideration of how the law regulates both cyber operations and the use of autonomous systems. This capability inherits from the cyber environment a special kind of secrecy, which makes its use particularly likely to escape censorship and make it a ghostly attack that spreads easily, quickly and at the lowest cost, as a hostile cyber system with a high degree of autonomy will interact with its environment, without constant external supervision, while remaining ideal within the framework of the higher-level goals it is programmed to achieve.

The latest statistics for 2024, prove that the world is heading towards more instability and that aggressive cyber has emerged from the traditional legal contexts, at least in proving the source and identity of the attacker, as well as how to deal with such situations, which pushes us as Arab countries to the need to adopt unified cyber diplomacy, in exchange for maximizing the human and financial resources allocated to cyber defence, and finally moving towards preparing specialized legal teams, to deal with such forms of unconventional aggression.

CONCLUSION

In conclusion, the marked increase in civilian participation in cyber attacks highlights a critical weakness under international humanitarian law, which requires decisive and swift action.

The reality imposed by the direct participation of civilians in hostile cyber operations can be summarized as follows:

New challenges emerge: The acceleration of cyberattacks presents a new dimension to the issue of civilian participation. In the digital sphere, distinguishing between the roles of civilians and combatants is made more difficult by cyber operations' anonymous and decentralized nature.

The need for legal innovation: Existing IHL frameworks may not fully address the complexities added by cyberattacks. New legal standards and definitions of cyber operations are needed to fill these gaps and better protect civilians while holding those involved accountable.

Need for a new definition of direct engagement: Develop a clear and new definition of direct cyber engagement to define the roles of civilians and combatants in cyber operations.

Accountability and investigation: Establish specialized international courts or bodies to adjudicate cases of cyberattacks, including the involvement of civilians in aggressive cyberattacks.

Enhanced frameworks: To better manage the challenges posed by civilian participation in cyberattacks, international cooperation must be strengthened, specialized legal frameworks established, and definitions of cyber roles and responsibilities clarified. This will help ensure that the principles of humanitarian protection are preserved and that the principle of distinction is effective as the conflict landscape evolves.

In short, while international humanitarian law has made progress in addressing civilians' participation in conventional armed conflicts, the rise of cyberattacks highlights the need to develop legal standards and frameworks to address the unique challenges posed by the digital age.

REFERENCES

[1] Additional Protocol I and II of 1977 to the Geneva Conventions of 1949.

[2] Ahmed Aubais Al-Fatlawi, International Humanitarian Law, Zain legal publishing, Lebanon, Beirut, 2019.

[3] Allan, Collin, Direct Participation in Hostilities from Cyberspace, Virginia Journal of International Law, 2013, Vol. 54, No. 1.

[4] Chang, Zen, "Cyberwarfare and International Humanitarian Law", Creighton International and Comparative Law Journal, Vol. 9 Issue 1. 2017. Available at: https://ssrn.com/abstract=2973182

[5] David Turns, Cyber warfare and the notion of direct participation in hostilities, Journal of conflict and security law, 2012, Vol. 17, No. 2.

[6] David Wallace, Shane Reeves, Trent Powellrect Participation in Hostilities in the Age of Cyber: Exploring the Fault Lines, Harvard National Security Journal, Vol. 12, 2021.

[7] Elin Blusi, Closing the 'Revolving Door' of Civilian Protection Direct Participation in Hostilities by Civilians and Organized Armed Groups,2022.

[8] Ezio di Nucci and Filippo Santoni de Sio Drones and Responsibility Legal, Philosophical, and Sociotechnical Perspectives on Remotely Controlled Weapons, Routledge First published 2016.

[9] Francois Delerue, Civilian Direct Participation in Cyber Hostilities, IDP Journal, University of Catalunya, 2014, Issue 19.

[10] Frederick de Molinenen, Handbook on the Law of War for the Armed Forces, ICRC, 2000.

[11] Frits Kalshoven, constraint on the waging of war: an introduction to IHL, 4th ed., Cambridge University Press, Cambridge, 2011.

[12] ICRC, "International Law relating to the Conduct of Military Operations, Collection of the Hague Conventions and Certain Other Treaties", Geneva, second edition, September September 2001.

[13] ICTY, Prosecutor v. Blaškić, Appeals Chamber, Judgment, Case No, (IT-95-14-A), 29 July 2004.

[14] ICTY, Prosecutor vs. Fatmir Limaj, case No: IT-03-66-PT para.509. Available at https://www.icty.org/en/case/limaj

[15] ICTY, The Prosecutor v. Stanislav Galic - Case No. IT-98-29-T Available at https://www.icty.org/x/file/Legal%20Library/jud_supplement/supp46-e/galic.htm last accessed 23-8-2024

[16] International Criminal Tribunal for the Former Yugoslavia, Kupreškić case, cited by John-Henkertz and Luizdozald-Beck, op. cit., rule 15.

[17] Israeli High Court of Justice, Targeted Killing Case, The Public Committee Against Torture in Israel v. The Government of Israel, (HCJ 769/02), Judgment of 11 December 2005.

[18] Jean-Marie Henckaerts and Louise Doswald-Beck, "Customary International Humanitarian Law", vol. I, Rules, ICRC, Brent Wright Advertising Press, Cairo, Egypt, 2007.

[19] Marco Sassoli and Lindsey Cameron, The Protection of Civilian Objects: Current State of the Law and Issues, de lege friend, 2006.

[20] Michael N. Schmitt and Liis Vihul, "Tallinn Manual 2.0 on International Law Applicable to Cyber Operations", 2nd ed, Cambridge University Press, Cambridge, 2017.

[21] Nils Melzer, Interpretive guidance on the notion of direct participation in hostilities under international humanitarian law, ICRC, First Arabic Edition, Regional Information Center, Cairo, 2010.

[22] 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, New York University Journal of International Law and Politics, 2010, Vol. 42, No. 3.

[23] Nishat Subah Maliha,Cyber Warfare: Challenges In The Application Of International Humanitarian Law To Virtual Conflict, Department of Law University of Dhaka,2020.

[24] Prescott, Jody M. Direct Participation in Cyber Hostilities: Terms of Reference for Like-Minded States? International Conference on Cyber Conflict (CYCON 2012). IEEE, 2012.

[25] Protocol on Prohibitions or Restrictions on the Use of Incendiary Weapons, Protocol III to the 1980 United Nations Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects.

[26] Schmitt, Michael N, The Interpretive Guidance on the Notion of Direct Participation in Hostilities: A Critical Analysis, Harvard National Security Journal, 2010, Vol. 1.

[27] Schmitt, Michael N., Deconstructing Direct Participation in Hostilities: The Constitutive Elements. New York University Journal of International Law and Politics, 2010, Vol. 42.

[28] Thamer Mohamed Ismail Al-Husseini, International Humanitarian Law vs. Intra-City Hostilities, A Study in the Principle of Feasible Precautions, PhD thesis submitted to Al-Alamein Institute for Graduate Studies, as part of the requirements for obtaining a doctorate in public law, Al-Alamein Institute for Graduate Studies, Republic of Iraq, 2023.

[29] the Hague Regulations Concerning the Laws and Customs of War on Land, The Hague, 1907.

[30] Toni PFANNER, Military Uniforms and the Law of War, in IRRC, No. 856, 2016.

[31] Top Cybersecurity Statistics for 2024, available at: https://www.cobalt.io/blog/cybersecurity-statistics-2024

[32] W. Hays Parks, 'Air War and the Law of War' (1990) 118 Air Force Law Review; R. Scott Adams, 'W. Hays Parks and the Law of War, 2020.

[33] Wallace, David A., and Shane Reeves. The Law of Armed Conflict's' Wicked' Problem: Levée En Masse in Cyber Warfare, International Law Studies Journal, U.S Naval College, Vol. 89,2013.

[34] Yves Sandoz et al, Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949, International Committee of the Red Cross, Martinus Nijhoff Publishers, Geneva, 1987.