The Challenge of Direct Participation between Ukraine and Russia: Civilization of Digital Warfare

Author: Eymen Ugur Saglam

Institution: Lumiere Education

The Challenge of Direct Participation between Ukraine and Russia: Civilization of Digital Warfare

Abstract

The use of digital technologies by civilians during the war between Russia and Ukraine has raised questions about whether or not they are "directly participating" in hostilities, and as a result, whether or not they are protected by IHL. While some politicians argue that citizens were victims who used technology in a way to save themselves, others argue that citizens who used technology were direct participants in war so they temporarily lose their immunity from attack, meaning that they could be struck anytime anywhere during war and this wouldn't be a crime. In light of this unresolved debate, this research paper asks the following questions: How does technology change the battlefield between Ukraine and Russia, and how does IHL apply to ordinary citizens involved in digital warfighting? Moreover, how can international law better protect civilians in digital conflict? This paper approaches these questions in a systematic way, which will help people to see real life cases in a more efficient way and consider the "problems'' and the "solutions'' at the same time by also providing ideas that a professional, the Ambassador of Ukraine to Turkiye, Vasyln Bodnar, shared with me during an interview we made for this research paper.

Keywords: Technology, development, change, civilians, IHL

Introduction

In February 2022, Russia launched a full-scale invasion of Ukraine. The war between them occurred after specific events that prepared the ground for their war. Specifically, after Ukraine's declared independence from Moscow with the fall of the Soviet Union, Ukraine was getting out of the Kremlin's orbit and started to focus on NATO and the European Union. Later, instead of choosing the EU, the new prime minister decided to revive economic ties with Moscow, triggering months of mass protests in Kyiv. Within days, armed forces seized parliament in the Ukrainian region of Crimea and raised the Russian Flag.

Russia's illegal annexation of Crimea in 2014 marked the beginning of the Russo-Ukrainian War. Since then, many specific events happened which raised tensions between Russia and Ukraine. Finally, in February 2022, Russia launched its full-scale invasion of Ukraine.

During the war, the effects of technology have been obvious. Specifically, the emergence of digital technologies has changed the nature of war and "digitalized" it. For example, the "Ukrainian IT Army" is composed of over 400,000 international and Ukrainian volunteer hackers,(Council on Foreign Relations, 2024) to target Russian infrastructure and websites. Many new concepts such as "Hacktivism" emerged with these developments. Apart from hacking, the role of social media has also played a role in digital warfare by creating a zone where everyone can share their opinions openly and actively. As a result, "civilianization" became a key

phenomenon in digital warfare. For example, Ukrainian citizens have used digital apps and other technological platforms to report to each other and Ukrainian authorities the locations of Russian soldiers.

This situation has presented the world with a new challenge. Under international humanitarian law (IHL), the body of law that (ICRC, 2022) seeks to limit the effects of armed conflict on civilians, militaries must distinguish (ICRC, n.d.-a) between "combatants" and "civilians" in conducting their operations to minimize the harmful effects of war on ordinary people. However, civilian immunity is not absolute. According to Additional Protocol 1 Art 51(3) of the Geneva Conventions (ICRC, 1977a), civilians are immune from being targeted (Opinio Juris, 2022) "unless and for such time as they take a direct part in hostilities."

The use of digital technologies by civilians (Harwell & Lerman, 2022a) support for the war effort has raised questions about whether or not they are "directly participating" in hostilities, and as a result, whether or not they are protected by IHL. While some politicians argue that citizens were victims who used technology in a way to save themselves, others argue that citizens who used technology were direct participants in war (ICRC, n.d.-a) so they temporarily lose their immunity from attack, meaning that they could be struck anytime anywhere during war and this wouldn't be a crime.

Literature Review

There is a broad existing literature on international law and digital warfare. It is accepted within the existing literature that international law governs the actions of the states around the world. Specifically, during war, their actions are guided by international humanitarian law, which is a set of rules that seek to limit the effects of armed conflicts. In addition it is also widely accepted that technology affects warfare and creates complicated situations under international law by changing the way in which war is fought.

Many works have been written on how technology affects the nature of warfare generally. To take one example, William Merrin's Digital War (Merrin, 2018) offers a general overview of the concepts of digital war, the media, the global public and warfare itself. The piece begins with the 1991 Gulf War, which was effective on many technological warfare developments. Later, it explains how the developments in the Gulf War were used in future wars. The book examines how technologies affected wars broadly and draws on major political events caused by the results of technology's effects on warfare. As it is seen, even though it focuses on technology and warfare relationship, it does not focus on how civilians act in such cases and doesn't really focus on the law part.

Moreover, civilian involvement in warfare has always been a feature of war. As a result, many articles exist about this case. For example, The Revolving Door of Modern Warfare: Civilian Direct Participation in Hostilities by Alessandro Silvestri (Silvestri, 2022) focuses on the concept of direct participation in hostilities (DPH), moreover, how civilians get involved in wars. The paper briefly explains how DPH

works and later it examines the principle of distinction by checking some examples related to civilian involvement. Overall, this piece aims to explain how IHL works and the mechanism of civilian involvement in wars. This article is a great example of how existing literature already explained the way civilian involvement is blurry at many points, yet, it doesn't contain examples or studies related to "digital war" and technology's effect on civilian involvement.

Finally, there is a lot of existing literature about the law that checks digital warfare. As an example, Cyber Wars: Applying Conventional Laws to War to Cyber Warfare and Non-State Actors by Shaun Roberts (HeinOnline, 2021) is focusing on the issues about the laws on cyber warfare and their gaps. Specifically focusing on the cyber attacks that Estonia suffered in 2007, this piece draws an overview about the existing law and its' appliance on cyber warfare. It gives some assumptions about how riskful these gaps in law and cyber attacks could be, such as assuming that John F. Kennedy International Airport in New York is suffering from cyber attacks. Seeing that digital warfare has brought broader targets, this paper focuses on the gaps and blurry conditions of existing law's appliance on digital warfare. Even though it gives examples of the gaps in law and explains the current legislative situation really well, no systematic overall observation of technology's effect on warfare and civilian involvement with technologies is given.

Afterall, these pieces are focusing on "narrow" issues and the existing literature needs articles that cover all those specific ideas systematically and gain an

easier way to show the reader about every corner of this issue and an overall broader information.

In sum, the blurry lines between citizens and combatants in digital warfare has generated debate among scholars about. Yet, even though a lot of pieces about technology and warfare currently exist, there is no paper that covers how technology affects the battlefield between Ukraine and Russia, how IHL applies to ordinary civilians involved in warfighting, and how the law could better protect the civilians in a systematic way. My paper approaches these questions in a systematic way, which will help people to see real life cases in a more efficient way and consider the “problems'' and the “solutions'' at the same time by providing a systematic overview. In doing so, this paper will fill a gap in the literature on this topic.

Argument and Outline

I argue that technology has changed the nature of warfare to the extent that some rules under IHL are not that effective anymore, specifically by raising involvement of civilians in warfare with the emergence of new digital technologies. Particularly focusing on Ukraine and Russia’s war, this paper uncovers how civilian involvement is rising in the light of new digital technologies. and to what extent distinction principles and civilian protection IHL is enough. In light of the gaps in

IHL, I also argue how IHL could be improved in future so that these complicated issues could be fixed.

To better understand the problem of Ukrainian civilians in the Russia-Ukraine war, the first section defines IHL and direct participation in hostilities in detail. The next section discusses the key ways in which technology is affecting the nature of digital warfare and civilian involvement in digital warfare. It focuses in particular on social media and disinformation campaigns, the role of civilians in gathering open source intelligence, cyber warfare and hacking. This step explains how civilians are being involved in war more than the past and presents real life examples about how the lines between civilians and combatants are getting more blurry with the developments in digital technologies. It also discusses the implications of civilian involvement in digital warfare for the principle of distinction, which explains what kind of different outcomes this phenomena has led to and how the principle of distinction is being affected by civilian involvement.

The last part defines existing protection of civilians under IHL and considers to what extent IHL is adequate to distinguish between civilians and combatants and protect civilians. Observing that there are existing gaps on IHL's appliance on digital warfare, the summary part presents how risky this challenge could be in the future if the gaps are not fixed immediately. It argues that if these kinds of debates can't find effective solutions, there might be aggressive debates between policymakers that would risk international collaboration. As long as these gaps exist under IHL, it will get harder to find solutions.

IHL and Direct Participation in Hostilities

To understand the problem of Ukrainian civilians in the Russia-Ukraine war, it is necessary to define International Humanitarian Law (IHL) as well as the concept of "direct participation in hostilities."

What is IHL?

Armed conflicts have the potential to inflict damage to nations and the world that can not be fixed in the future. To prevent states from acting however they want in the international arena, there is the need for international rules that can control their actions. This is why states established IHL. According to the International Committee of the Red Cross (ICRC) advisory service on IHL, it is a "set of rules which seek, for humanitarian reasons, to limit the effects of armed conflict.(ICRC, 2022) It protects people who are not or are no longer participating in the hostilities and restricts the means and methods of warfare." IHL is also known as the law of war or the law of armed conflict. It is part of international law, which is the body of rules governing relations between States.

IHL applies only to armed conflict, and does not cover any internal tensions or disturbances. The law applies only once a conflict has begun, and then equally to all sides regardless of who started the fighting. IHL distinguishes between international and non-international armed conflict(RULAC, n.d.). International armed conflicts are those in which at least two States are involved. They are subject to a wide range of rules under IHL, including those set out in the four Geneva Conventions and Additional Protocol I.(ICRC, 2024a) Non-international armed

conflicts take place within the territory of a single State, involving either regular armed forces fighting groups of armed dissidents, or armed groups fighting each other. A more limited range of rules apply to internal armed conflicts and are laid down in Article 3 common to the four Geneva Conventions(ICRC, 1949) as well as in Additional Protocol II.(ICRC, 1977b)

It is important to differentiate between international humanitarian law and human rights law. While some of their rules are similar, these two bodies of law have different appliance areas and they contain different treaties. A key difference between both is that Human Rights Law applies in peacetime, and many of its provisions may be suspended during an armed conflict while IHL applies only during armed conflict and focuses on wartime.

What Does IHL Cover?

According to the ICRC, IHL covers two areas:(ICRC, 2020) (1) the protection of those who are not, or no longer, taking part in fighting; and (2) restrictions on the means of warfare – in particular weapons – and the methods of warfare, such as military tactics.

IHL protects those who do not take part in the fighting,(Diakonia, n.d.) such as civilians and medical and religious military personnel. It also protects people who have stopped to take part in war, such as wounded combatants and prisoners of war. These people are seen as mentally or physically traumatized so they need to be respected under the conditions they've gone through. They also enjoy legal guarantees. They must be protected and treated humanely in all circumstances, with no distinction.

The distinction between members of the armed forces and civilians(ICRC, 2024b) is the key element of IHL. The duty of IHL is the prohibition on the targeting of civilians. Militaries must distinguish between combatants and civilians – the only two categories in the Geneva Conventions. However, civilian immunity is not absolute: according to Additional Protocol 1 Art 51(3)(ICRC, 1977a), civilians are immune from being targeted "unless and for such time as they take a direct part in hostilities."

Importantly, it is not always easy to distinguish between civilians and combatants because sometimes civilians engage in acts that support the war effort. This raises questions about whether or not they are directly participating in hostilities. Direct participation in hostilities means determining when civilians' actions compromise their otherwise protected civilian immunity.(Bosch, 2014) According to the ICRC's Interpretive Guide, before an act can be referred to as direct participation in hostilities it must meet three criteria(Melzer, 2009):

(1) “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);”

(2) “There must be a direct causal 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);” and(3) The act must be specifically designed to directly cause the required threshold of harm in support of a party to the conflict and to the detriment of another (belligerent nexus).

According to IHL, civilians “enjoy complete immunity against attack for such time as they abstain from any direct participation in hostilities.” However, as soon as civilians give up their civilian immunity by participating directly in hostilities, their actions also make other civilian victims become targets to"erroneous or arbitrary attack(ICRC, 2024c).” As a consequence, in order to discourage civilians from abusing their civilian immunity, IHL ignores the temporary suspension(ICRC, n.d.-a) of their civilian immunity against direct targeting, for so long as they participate directly in hostilities. Even if their civilian immunity is temporarily suspended, this has no effect on their primary IHL status as civilians. At no time do they lose their civilian status and become a combatant. Moreover, when they leave their participation, they gain full civilian immunity against attack.

Notably, his temporary suspension of a civilian's immunity against direct attack is afforded only to "civilians who participate in hostilities on a spontaneous,

unorganized or sporadic basis.(ICRC, n.d.-b)" Consequently, once it has been decided that a civilian has carried out a specific act which amounts to direct participation in hostilities, the next level of investigation must address determining the beginning and end of the loss of civilian immunity.

The Changing Character of War: Rising Civilian Involvement in Digital Warfare

The previous section has covered what IHL is and the idea of direct participation in hostilities. This section will discuss the effects of technology on the battlefield and how civilian involvement is challenging the principle of distinction and the idea of direct participation in hostilities.

Civilians' participation in wars have been a fact of war throughout history. They've joined wars to a greater or lesser degree whether being part of arms production or by providing support to conflicts in many categories such as economic or political support. Usually, they were not attending at the battlefront and only a small number of civilians were actually involved in the part of military operations. Under these circumstances, it was much easier to determine who was a combatant, and who was a civilian protected under IHL from direct attack.

In the past few decades, battlefields have become less distinct with fighting taking place in civilian population centers.(ICRC, 2017) In particular, the emergence of new digital technologies has created a space where civilians participate and affect the war(Mačák, 2023a) much more. With the effects of technological developments, civilians have been increasingly involved in activities more closely related to the conduct of hostilities, blurring the distinction between civilian and military

functions(Mačák, 2021) Cyber warfare does not only create a non-physical virtual area, it also facilitates the involvement of civilians in warfare(Mačák, 2023b). Since digital war is virtual and much more accessible than before, civilians tend to attend more into related areas and debates.

In particular, this phenomenon has been widely observed in the Russia-Ukraine war, though according to the ambassador of Ukraine to Turkiye " Russian aggression against Ukraine has indeed highlighted the importance of digital technologies in modern conflicts. However, digital warfare is a phenomenon that has been developing over the past decades and was already noticeable in other conflicts. Notably, the conflicts in Syria, Iraq, and Libya demonstrated how digital platforms are used to disseminate information, propaganda, and coordinate various actions on the battlefield."

Nonetheless, Russia's war has highlighted the importance of digital technologies in conflict on the global stage. Many journalists described the war between Russia and Ukraine as the "most internet accessible war(Harwell & Lerman, 2022a)" and also as the "most viral war(The Economist, 2022)". Social media domain and sharing of information can be defined in different ways. For example, John Spencer, head of urban warfare studies at the U.S. Military Academy's Modern War Institute, said "This is kind of the new way of warfare, there's no more going away to war. We're all with Ukraine right now." After he tweeted(Spencer, 2022) a guide for how "civilian resistors" could strike fear in the hearts of attacking Russians,

Ukrainian users translated it almost immediately, sharing it across Telegram and making digital fliers.

Many people believe that the internet has opened a new dimension of war. Afterall, it has increased blurry lines between civilians and combatants in many areas and created a challenge for the world. In particular, I argue there have been three main developments: social media and disinformation campaigns, open source intelligence sharing, hacker activities.

Civilian Involvement in Disinformation Campaigns

Social Media and Information Warfare:

Maybe it existed before the newest technologies as a more familiar concept but, social media has changed a lot too. Considering that everyone is free to express their feelings, thoughts and advice on anything, social media platforms have become widely open to manipulation. This situation has affected the nature of war, too. Social media platforms created a zone where everyone could share their opinions openly and actively. It also helped people to feel like they could contribute to the fight. Many key examples are seen in the war between Russia and Ukraine. Solomiia Shalaiska, a Kyiv-based graphic designer, said she felt helpless(Hillsboro Globe, n.d.) until she started posting pro-Ukraine rally images on an Instagram page she previously used for art and design. “It’s very important to strengthen the national spirit in Ukraine, that’s why people are doing memes and encouraging images,” she said in an Instagram message. These actions may target Russian people and even

spread a high amount of wrong information which makes social media a risky place during the digital war.

Another example is being observed in the war between Israel and Palestine. The effect of misinformation on the world is at a critical level because, with the rise of social media, it is much harder to know which information is correct and which is wrong. For example, in a 28 second video(Frenkel, 2021), which was shared by a spokesman for Prime Minister Benjamin Netanyahu, Palestinian militants are shown while attacking Israelis in an area which is filled with civilians. At least that was what the spokesman said. Yet, the video that was shared hundreds of times, was not even from Gaza. It was not even from the week that the video was shared by the spokesman! Instead, the video that he shared, which can be found in many video hosting sites, was actually from 2018. Moreover, according to the captions of the video, the images are most probably from Syria or Libya. This is just one example of the disinformation campaigns. As people get more involved in war with their opinions, social media is going to be a riskier domain day by day.

The Role of Civilians in Gathering Open Source Intelligence

In addition to participating in disinformation campaigns, the invasion of Ukraine has created a massive amount of digital data that could refer to potential direct participation cases. Ordinary civilians and activists are trusting their smartphones to collect and keep photos and videos(Bergengruen, 2022). Citizen researchers are investigating online to identify and verify atrocities and perpetrators(Bellingcat, n.d.).

Open-source investigating and use of digital information comes with many risks. For example, a 2021 report published by the Stanley Center(Stanley Center, 2022) focused on the risks for collateral harm(Stanley Center, 2022) stemming from open-source journalism. One reporter described a story that he was writing about video footage from a missile strike in the Middle East(War on the Rocks, 2022): "We wanted to include the video in our reporting. But based on the video, it wouldn't be hard to figure out which building, apartment, or window our contact was standing in when filming. That could get the person arrested or bring harm to a family. In this case, we didn't publish the video with our reporting." Just like open information could bring support to victims, it could create a risky situation because information is really easy to find online in today's world. These examples show that "sharing information" might not go as planned, and make civilians liable to be harmed.

Another example is the Diaa app. In early 2020, prior to the war, Ukraine launched the Diia app(The Guardian, 2023) as a good government initiative to make it easier for citizens to renew licensing permits, pay for parking tickets, and report potholes. However, something interesting happened later. We saw another example of civilian involvement in digital warfare after the invasion in 2022, when the Ukrainian government updated the app and turned it into a digital platform that would serve as "the ears and eyes of the Ukraine army". "After hostilities broke out we thought: what did the citizens of Ukraine need? They needed money, protection, and compensation when rockets hit their house," Federov said. Now, for example, the app allows victims of Russian bombings to apply for funds to repair damaged buildings and to continue to listen to the radio during blackouts. It also permits the

creation of a digital “evacuation document” combining all personal information in one place to “accelerate identification at checkpoints”; “e-aid” financial support(X, 2023) for small businesses “to keep the economy going” and “e-enemy” a chatbot to report the location of Russian soldiers. The fact that civilians could share any document or information means that they could share Russian soldiers’ locations, images or identities, which they did. Afterall, these actions have the risk to activate a direct participation, which risks Ukrainians on this field to lose their immunity from attacks.

Cyber Warfare and Hacking: An Increasing Role for Civilians

A third way civilians have increasingly become involved in digital warfighting is “hacktivism.” Importantly, the widespread participation of ‘hacktivists(Reuters, 2024)’ in hostile cyber operations raises questions about their status under IHL. While civilians are normally immune from attack, they lose that immunity for such a time that they directly participate in hostilities (DPH). As it was argued in the first two parts, there are some complications about IHL’s appliance on DPH cases. The notion of harm is critical for DPH: since harm does not have to involve kinetic effects, according to Professor Aurel Sari(Sari, 2023), participation in cyber operations that are likely to inflict non-physical harm on an adversary (such as intelligence gathering, degrading their communications or adversely affecting command and control through ruses) may count towards DPH. When the argument is about physical activities that are counted as “attack” under IHL, it is easier to determine who directly participates in a hostile, yet, when it comes to digital space

it is highly argued among politicians whether those “volunteer hackers'' are activating the DPH condition and should lose their immunity from attacks under IHL or not.

Nevertheless, a more complicated part occurs on the Ukraine side of digital zones. Just like Russia, Ukraine also has volunteer hackers which are actually organized by the Ukrainian government. The “Ukrainian IT Army” is composed of over 400,000 international and Ukrainian volunteer hackers(Council on Foreign Relations, 2024), to target Russian infrastructure and websites. The army was created by Ukrainian Minister of Digital Information, Mykhailo Fedorov(Ukrainian Gov’t, n.d.), who sent a tweet with a link to a telegram channel that urged volunteers to “use any vector of cyber and [distributed denial of service] attacks on Russian resources(Tidy, 2022).” The initial post that he sent provided 31 Russian banks, commercial establishments, and government websites for targeting. The graphic designer mentioned above, Solomiia Shalaiska, also mentioned that(Harwell & Lerman, 2022a)she has joined the nation’s nascent “IT army(Council on Foreign Relations, 2024)”of volunteer hackers.

There are many other cases where it is seen that civilians enter the fray by providing tips and locations of one of the hostilities, which puts them into the “gray zone(Steer, 2023)” where it can not be decided whether they lose their immunity under IHL or they won't. For example, upwards of 1000 civilian drones contribute to Ukraine’s defense by surveilling Russian assets from the air and relaying crucial information to Ukrainian military units for artillery strikes(Financial Times, 2024a).

Many observers believe that “hacktivists” can still impact the nature of war to a certain level if informal groups of foreign “hacktivists”are keen to help Ukraine. For example, according to John Thornhill (Financial Times, 2024b), says, “When they play defense, these “white hat” hackers (Financial Times, 2024c) can help to find and plug holes in Ukraine’s digital networks. But if they participate in disinformation campaigns or cyber attacks on Russian targets, there may be unpredictable results.”.

On the other hand, the director of the Citizen Lab at the University of Toronto, Ronald Deibert (University of Toronto, n.d.), takes a different point of view. According to Deibert,“It is understandable why Ukrainians who are defending their homes and lives would reach for any possible tool to defend themselves,” But that does not mean all norms and rules are suspended for everyone else: “If you’re going to get involved, you better understand the consequences. “Consequences” might mean several things but most probably it cites direct participation, which will make Ukrainian civilians lose their immunity from attacks under IHL.

Implications of Civilian Involvement in Digital Warfare for the Principle of Distinction

These phenomena have led to different outcomes. On the one hand, it has potentially saved lives: Ukrainians have raced to spread defensive strategies, plot escape routes and document the brutality of a raging clash (Bailey, 2024). Some expect that the phone footage recorded in recent years could play a critical role in investigating war crimes after the war ends. On the other hand, just as it potentially

saved lives, the information that was shared has also created the risk of civilians losing their immunity from attacks under IHL(ICRC, 1977b).

Specifically, the digitalization of warfare has created a mechanism where civilians can easily be involved in warfare and conflicts, making it more difficult to distinguish between civilians and combatants. With the involvement of civilians in warfare through the help of new technologies, cyber areas and the digitalized world has turned into a “gray zone.” This has created uncertainty as to how the principle of distinction, the cornerstone of IHL(ICRC, 2024b), should be implemented in the reality of present military operations.

For example, a problem arises if armed actors do not distinguish themselves from civilians during operations, or when they act as "farmers by day and fighters at night". This means that even if they look like civilians at first sight from the outside, they might actually be direct participants involved in war. As a consequence, enemy armed forces become unable to properly identify their opponent, and peaceful civilians are more likely to fall victim to arbitrary targeting.

Let’s look at two other examples specifically focusing on the situation between Israel and Gaza. Firstly, the case about Al-Jaala Tower(Wikipedia, 2024) simply exemplifies the risks of civilian buildings being used as military bases. Al-Jaala was not actually a military tower, quite the opposite, it was a building that civilians lived and had offices in. The principle of distinction requires certain distinction between civilians and combatants. Yet, the situation gets complicated when a military base is created in a civilian building. Israel powers detected that

there were Palestinian military powers inside so they supported the idea that the tower could be striked and they did so. This situation clearly presents an example about how hard it might be to identify civilians when technology enters the fray and blurs the lines.

A final example concerns the Hamas group in Gaza. It's hard to figure out exactly what military activities Hamas was doing in these civilian buildings(Haque, 2021) Since there's no clear public evidence showing that the al-Jalaa Tower was used for military operations, it’s difficult to judge if the rule about keeping civilians safe was followed. This case highlights another big problem that principle of distinction faces when it comes to cyber domains. In modern terms of warfare, especially with cyber warfare, where actions are often secret and hard to track, it becomes much harder to identify who gets involved in such military operations, furthermore, who is a combatant and who is not. This uncertainty makes it tougher to hold people responsible for breaking the rules, especially when civilians are hurt because the principle of distinction gets affected by technologies and becomes complicated.

Moreover, in light of increasing civilian involvement in digital warfare it is unclear how IHL distinguishes them from combatants and how it protects them. IHL says that civilians must be protected under the law, "unless and for such time as they take a direct part in hostilities". However, neither the Geneva Conventions nor their Additional Protocols provide a definition of what conduct amounts to direct participation in hostilities. The modern challenge, according to the ICRC, is thus to

provide clear criteria for the distinction not just between civilians and the armed forces, but also between peaceful civilians and civilians who directly participate in hostilities. Specifically, the ICRC believes three key questions need clarification(ICRC, 2017):

(1) Who is considered a civilian for the purposes of conducting hostilities? (2) What conduct amounts to direct participation in hostilities? (3) What are the precise modalities according to which civilians directly participating in hostilities lose their protection against direct attack?

In sum, rising civilian involvement in digital warfare has clear effects on the principle of distinction. As a result, the lines between civilians and combatants become more blurry day by day. Nonetheless, even though there are clear gaps about how the law applies to civilians involved in digital war, it is still useful to examine what existing scholarship says about the protection of civilians under IHL.

Adequate Protection? Examining Existing Protection of Civilians Under IHL

The previous section has covered the ways civilians become involved in warfare on digital space, moreover, the implications of rising civilian involvement in digital space on the principle of distinction. This section will now examine to what extent IHL currently protects those who are not identified as either a direct participant or not(ICRC, 2017).

A useful place to start is examining how IHL applies to cyberspace. just like every other conflict, IHL applies to the cyber domain, too. However, despite the general acknowledgement that international law applies to cyberspace, there are doubts about the extent to which existing international rules or principles apply to this new area of state activity. Since new technologies create new platforms, it has become necessary for IHL to be updated and synchronized with new digital zones. Some politicians and scholars argue that the law does not apply to cyber spaces. This idea depends on two assumptions(Akande et al., 2021). First, existing international law can only apply in cyberspace if supported by cyber specific evidence and opinio juris(Cornell Law, n.d.). Second, some rules that reflect international law obligations have been described as 'voluntary, non-binding norms of responsible state behavior(Leiden University, n.d.)' in cyberspace.

The first way to evaluate how IHL currently protects civilians involved in digital warfighting is to look at how the law applies to cyberspace. With the entrance of cyberspace into our lives, cyber operations and digitized warfare has become a reality of today's armed conflicts. According to ICRC, there is no question that IHL applies to cyber operations during armed conflict just like it applies to any other operation. However, the fact that cyberspace is a new domain just like air, land and outer space; but it is human made and not like the others, it lets civilians enter the war more than any other domain.

Yet, how effective IHL is in practice(Rushing, 2023)in protecting civilians in cyberspace is questionable. Arguments about when IHL apply should always

consider that, according to the ICRC, IHL applies only in case of any 'threat or use of force' or an "armed attack" under the UN Charter. To determine when IHL applies to digital warfare and cyber operations, it is necessary to differentiate between the following cases(ICRC, n.d.-c):

1. "When a cyber operation is carried out by one State against another in conjunction with or in support of classic 'physical' or 'kinetic' military operations in the context of an existing armed conflict, IHL applies to such operations."

2. "If – outside an existing armed conflict – a cyber operation is the only means by which hostile actions are undertaken by one State against another State, the law is unsettled as to whether such cyber operation could bring into existence an international armed conflict as defined under Article 2 common to the Geneva Conventions."

Even though it seems great on paper, there are blurry lines where it is sometimes argued that whether IHL protection on digital warfare is enough for civilians or not(Mačák, 2023a). This situation is mostly caused by civilians being involved in warfare more than usual with the emergence of new technologies and changing character of the warfare, as the following section will discuss further.

In sum, the issue of IHL's appliance on digital warfare is a highly debated topic. Current debates continue being argued about the amount of IHL's appliance in digital warfare but it is clearly seen that the law needs to be settled and updated considering today's world and current trends. The issue of information security has been on the UN agenda since 1998(UNODA, 2024), and since then many steps were

taken about many different concepts such as cyber operations against covid-19 vaccines(Oxford Institute, 2020). Yet, it is clearly observed that many steps must be taken about the civilianization of digital warfare and the results of this situation such as the complex direct participation issue.

Everything considered, international law lacks distinction certainty between civilians and combatants, so, it must be noted that IHL does not require enough protection for civilians when it comes to modern issues caused by new digital technologies. IHL protects civilians in the digital domain just as other domains, but since the world is changing in the light of new technologies, IHL needs to be updated according to these modern digital challenges.

Generally, international actors are arguing that IHL must be arranged according to digitalized warfare, yet, there are no concrete solutions that would solve the problems. It is clearly seen that IHL's appliance to civilians is not enough to protect them from the blurry lines that are created by digitized warfare. Crucially, this lack of protection creates ground for aggressor states to benefit from these blurry lines.

When it comes to the solutions to fix these gaps, there are no answers. International actors today are having many debates on possible solutions. If an effective solution is not found soon, protection of the civilians in the future will be an extremely risky challenge for the world. Considering how fast technology improves, the nature of warfare will continue to change really fast and international elements like the IHL should be arranged and updated according to the

developments in the modern world. Otherwise, the gaps could create terrifying problems and situations for civilians in future.

Conclusion

This paper examined how civilians are becoming involved in war with the emergence of new digital technologies and how IHL applies to civilians involved in digital warfighting. Focusing specifically on the Russia-Ukraine war, the paper discussed how civilians are being involved in war with the help of technological developments. It also reviewed the concept of IHL and direct participation in hostilities, and existing civilian protection under IHL.

This article argued that digital technologies have changed the balance of warfare. Many new phenomena have entered our lives and digital warspace. With the changing character of war, a key finding of this paper is that civilians are becoming involved in digital warfare more than ever, and that this situation raises many questions about how the lines between civilians and combatants are changing. Even though IHL contains many protection laws for civilians, it is seen that IHL lacks distinction of roles in warfare and civilian protection when it comes to digital war. In light of these observations, the paper found that IHL must be rearranged according to the needs of civilian protection and distinction in the effect of digital technologies. Seeing rising civilian involvement caused by new technologies and that there are some gaps about IHL on its appliance in digital warfare, this challenge should be fixed as soon as possible because in the future this situation is going to create much worse cases.

In sum, this article draws out a new path about the challenge of civilian involvement caused by new technologies in war. In the light of gaps this paper uncovered, future research should explore how the gaps in IHL could be fixed in the future and it must be discussed considering the importance of human life and the urgency of this issue by international actors in order to prevent worse situations from emerging. Vasyl Bodnar, the ambassador of Ukraine to Turkiye, informed me that international actors have proposed four primary solutions to resolve these issues during an interview we had: developing the international cyber norms, updating the Geneva Conventions, Strengthening international cooperation, and protecting human rights in digital warfare.

First, developing the international cyber norms is important because these norms would aim to prevent certain actions, such as targeting critical civilian infrastructure or using cyberattacks to disrupt essential services like healthcare and water supply. As an example that was given by Ambassador Vasyl Bodnar, there have been reports of GPS signal jamming and other forms of electronic warfare used by Russian forces in Ukraine. In addition, cyberattacks have targeted Ukraine's transportation and energy infrastructure, aiming to create chaos and hinder military and civilian logistics.

Second, updating the Geneva Conventions should be considered as a solution and legal experts are considering how to update the Geneva Conventions and other international humanitarian law (IHL) frameworks to explicitly include protections against cyber warfare. Ambassador of Ukraine to Turkiye, Vasyl Bodnar, says that

this would involve defining what constitutes a cyberattack, determining the applicability of IHL to cyber operations, and clarifying the responsibilities of states in preventing and responding to such attacks. Russia's use of cyber operations to disrupt Ukraine's military communications highlights the need to update the Geneva Conventions to address the legality and limitations of cyber warfare.

Third, strengthening international cooperation plays a major role and enhanced international cooperation is being proposed to improve the sharing of information and best practices among countries to better protect against cyber threats. Ambassador Vasyln Bodnar says that this includes collaboration between states, international organizations, and private sector entities to enhance cybersecurity and build resilience against digital attacks.

Last but not least, there is also a push to ensure that human rights are protected in the context of digital warfare. This includes addressing issues such as privacy, freedom of expression, and access to information, particularly in situations where digital technologies are used to control or manipulate populations.

Acknowledgments:

I would like to express my sincere gratitude to Gwendolyn Whidden from Oxford University for their invaluable mentorship, insightful feedback, and continuous support throughout the development of this research.

References

Akande, D., et al. (2021, January 2). *Old habits die hard: Applying existing international law in cyberspace and beyond*. EJIL. https://www.ejiltalk.org/old-habits-die-hard-applying-existing-international-law-in-cyberspace-and-beyond/

Bailey, S. (2024, April 8). *Gen Z looks for ways to help as war in Ukraine continues - The Threefold Advocate*. John Brown University. https://advocate.jbu.edu/2022/03/10/gen-z-looks-for-ways-to-help-as-war-in-ukraine-continues

Bellingcat. (n.d.). *Ukraine*. https://www.bellingcat.com/tag/ukraine/

Bergengruen, V. (2022, April 18). *How Ukraine is crowdsourcing digital evidence of war crimes*. *Time*. https://time.com/6166781/ukraine-crowdsourcing-war-crimes/

Bosch, S. (2014). The international humanitarian law notion of direct participation in hostilities – A review of the ICRC interpretive guide and subsequent debate. *Potchefstroom Electronic Law Journal (PELJ)*. North West University. https://www.scielo.org.za/scielo.php?script=sci_arttext&pid=S1727-37812014000300006

Council on Foreign Relations. (2024). *Connect the dots on state-sponsored cyber incidents – Ukrainian IT Army*. Council on Foreign Relations. https://www.cfr.org/cyber-operations/ukrainian-it-army

Cornell Law. (n.d.). *Opinio juris (international law)*. Legal Information Institute. https://www.law.cornell.edu/wex/opinio_juris_(international_law)

Diakonia International Humanitarian Law Centre. (n.d.). *Protected persons under IHL*. https://www.diakonia.se/ihl/resources/international-humanitarian-law/protected-persons-under-ihl/

Financial Times. (2024a). *Ordinary Ukrainians wage war with digital tools and drones*. https://www.ft.com/content/58a5b1a6-bb92-4008-a919-ae6bf73a5419

Financial Times. (2024b). *What an epic 18th-century scientific row teaches us today*. https://www.ft.com/john-thornhill

Financial Times. (2024c). *Ukraine is winning the information war against Russia*. https://www.ft.com/content/2a11a507-80a3-4da5-9eee-4dafa4a7ee6e

Frenkel, S. (2021, May 17). Lies on social media inflame Israeli-Palestinian conflict. *International New York Times*. Gale Academic OneFile. https://link.gale.com/apps/doc/A661972114/AONE?u=anon~d5468b2b&sid=googleScholar&xid=27b56311

Haque, A. A. (2021, June 2). *The IDF's unlawful attack on Al Jalaa Tower*. Just Security. https://www.justsecurity.org/76657/the-idfs-unlawful-attack-on-al-jalaa-tower/

Harwell, D., & Lerman, R. (2022, March 1). *How Ukrainians have used social media to humiliate the Russians and rally the world*. *The Washington Post*. https://www.washingtonpost.com/technology/2022/03/01/social-media-ukraine-russia/

HeinOnline. (2021, March 8). *About*. https://heinonline.org/HOL/LandingPage?handle=hein.journals%2Fnkenlr41&div=31&id=&page=

Hillsboro Globe. (n.d.). *Ukrainian teens use social media combat Russian president's invasion of Ukraine*. https://hillsboroglobe.com/16958/news/ukrainianinfluencers/

International Committee of the Red Cross. (1949). *Geneva Convention I, Article 3*. IHL. https://ihl-databases.icrc.org/en/ihl-treaties/gci-1949/article-3

International Committee of the Red Cross. (1977a). *Protocol I, Article 51*. IHL. https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-51

International Committee of the Red Cross. (1977b). *Protocol II, Article 13*. IHL. https://ihl-databases.icrc.org/en/ihl-treaties/apii-1977/article-13

International Committee of the Red Cross. (2017, November 30). *Civilian 'direct participation in hostilities': Overview*. https://www.icrc.org/en/document/civilian-direct-participation-hostilities

International Committee of the Red Cross. (2020). *What is international humanitarian law?* https://www.icrc.org/en/doc/assets/files/other/what_is_ihl.pdf

International Committee of the Red Cross. (2022, July 5). *What is international humanitarian law?* https://www.icrc.org/en/document/what-international-humanitarian-law

International Committee of the Red Cross. (2024a, June 28). *The Geneva Conventions and their commentaries*. https://www.icrc.org/en/document/geneva-conventions-1949-additional-protocols

International Committee of the Red Cross. (2024b, June 25). *Direct participation in hostilities*. https://www.icrc.org/en/law-and-policy/direct-participation-hostilities

International Committee of the Red Cross. (2024c, June 27). *Direct participation in hostilities: Questions & answers*. https://www.icrc.org/en/article/direct-participation-hostilities-questions-answers

International Committee of the Red Cross. (n.d.-a). *Customary IHL Rule 1*. IHL. https://ihl-databases.icrc.org/en/customary-ihl/v1/rule1

International Committee of the Red Cross. (n.d.-b). *Interpretive guidance on the notion of direct participation in hostilities*. ICRC Casebook. https://casebook.icrc.org/case-study/icrc-interpretive-guidance-notion-direct-participation-hostilities

International Committee of the Red Cross. (n.d.-c). *When does international humanitarian law apply to the use of force?* https://www.icrc.org/sites/default/files/wysiwyg/war-and-law/01_when_does_ihl_apply-0.pdf

Leiden University. (n.d.). *Voluntary, non-binding norms for responsible state behaviour in the use of information and communications technology: A commentary*. https://www.universiteitleiden.nl/en/research/research-output/governance-and-global-affairs/voluntary-non-binding-norms-for-responsible-state-behaviour-in-the-use-of-information-and-communications-technology-a-commentary

Mačák, K. (2021, November 5). *Unblurring the lines: Military cyber operations and international law*. Taylor & Francis. https://www.tandfonline.com/doi/epdf/10.1080/23738871.2021.2014919

Mačák, K. (2023). *Civilianization of digital operations: A risky trend*. Lawfare. https://www.lawfaremedia.org/article/civilianization-digital-operations-risky-trend

Melzer, N. (2009). *Interpretive guidance on the notion of direct participation in hostilities under international humanitarian law*. ICRC. https://www.oas.org/es/sla/ddi/docs/publicaciones_digital_XXXVI_curso_derecho_internacional_2009_Nils_Melzer.pdf

Merrin, W. (2018, August 2). *Digital war: A critical introduction*. Taylor & Francis. https://www.taylorfrancis.com/books/mono/10.4324/9781315707624/digital-war-william-merrin

Opinio Juris. (2022, September 13). *Military information sharing by Ukrainian citizens in the digital environment: DPH? – Blurring of lines between civilian and military actors in Ukraine*. https://opiniojuris.org/2022/09/12/military-information-sharing-by-ukrainian-citizens-in-the-digital-environment-dph-blurring-of-lines-between-civilian-and-military-actors-in-ukraine/

Oxford Institute for Ethics, Law and Armed Conflict. (2020, July 31). *Safeguarding the COVID-19 vaccine research*. Oxford.

Reuters. (2024, January 4). *Exclusive: Russian hackers were inside Ukraine telecoms giant for months – Cyber spy chief*. https://www.reuters.com/world/europe/russian-hackers-were-inside-ukraine-telecoms-giant-months-cyber-spy-chief-2024-01-04/

RULAC. (n.d.). *Classification*. https://www.rulac.org/classification#collapse1accord

Rushing, E. (2023, March 7). *Towards common understandings: The application of established IHL principles to cyber operations*. *Humanitarian Law & Policy Blog*. https://blogs.icrc.org/law-and-policy/2023/03/07/towards-common-understandings-the-application-of-established-ihl-principles-to-cyber-operations/

Sari, A. (2023). *International law and cyber operations: Current trends*. Council of Europe. https://rm.coe.int/64th-cahdi-pr-aurel-sari-presentation/1680aaaf48

Silvestri, A. (2022, December 16). *The revolving door of modern warfare: Civilian direct participation in hostilities*. University of Western Australia Research Repository. https://research-repository.uwa.edu.au/en/publications/the-revolving-door-of-modern-warfare-civilian-direct-participatio

Spencer, J. (2022, February 26). *So I've been asked what my advice would be to civilian resistors in Ukraine...* [Tweet]. X (formerly Twitter). https://mobile.twitter.com/SpencerGuard/status/1497583307504046087

Stanley Center. (2022). *Feeling the burden: Ethical challenges and practices in ….* https://stanleycenter.org/wp-content/uploads/2022/01/NWRPT-FeelingtheBurden_122-v2.pdf

Steer, C. (2023, January 30). *International humanitarian law in the 'grey zone' of space and cyber*. Centre for International Governance Innovation. https://www.cigionline.org/articles/international-humanitarian-law-in-the-grey-zone-of-space-and-cyber/

The Economist. (2022). *The invasion of Ukraine is not the first social media war, but it is the most viral*. The Economist Newspaper. https://www.economist.com/international/the-invasion-of-ukraine-is-not-the-first-social-media-war-but-it-is-the-most-viral/21808456

The Guardian. (2023, May 26). *Meet Diia: The Ukrainian app used to do taxes … and report Russian soldiers*. Guardian News and Media. https://www.theguardian.com/world/2023/may/26/meet-diia-the-ukrainian-app-used-to-do-taxes-and-report-russian-soldiers

Tidy, J. (2022, March 7). *Twitter is part of our war effort – Ukraine minister*. *BBC News*. https://www.bbc.com/news/technology-60608222

United Nations Office for Disarmament Affairs. (2024). *Developments in the field of information and telecommunications in the context of international security*. https://disarmament.unoda.org/ict-security/

University of Toronto. (n.d.). *Faculty: Department of Political Science*. https://politics.utoronto.ca/faculty/profile/28/

Ukrainian Government. (n.d.). *Mikhaylo Fedorov*. https://www.kmu.gov.ua/en/profile/mikhaylo-fedorov

War on the Rocks. (2022, December 6). *Disentangling the digital battlefield: How the internet has changed war*. https://warontherocks.com/2022/12/disentangling-the-digital-battlefield-how-the-internet-has-changed-war/

Wikipedia. (2024, July 27). *Destruction of the Al-Jalaa building*. Wikimedia Foundation. https://en.wikipedia.org/wiki/Destruction_of_the_al-Jalaa_Building

X. (2023). *Lisa O'Carroll post*. https://x.com/lisaocarroll/status/1661771089679196161