LAWFARE

INTERNATIONAL LAW: LOAC: DISTINCTION

Civilianization of Digital Operations: A Risky Trend

By **Kubo Mačák**, **Mauro Vignati** Wednesday, April 5, 2023, 8:16 AM

For more than two decades, states have used cyber capabilities for military purposes. There are two main types of cyber operations: those aimed at obtaining confidential information for strategic advantage (presence based) and those that seek destructive or disruptive impact (events based).

The digital operational range of states, however, is no longer limited to cyber operations. Echoing the global trend toward the digitalization of our societies, armed forces around the world are developing innovative strategies to utilize the digital sphere in more complex and broader ways than ever before.

These developments are putting renewed pressure on the established international legal principles that constrain what is permissible in war. Such principles—which, according to a consensus in the international community, include the principles of humanity, necessity, distinction, and proportionality—are part of international humanitarian law (IHL), a body of law that sets important limits on the conduct of parties to armed conflicts.

This article focuses on the principle of distinction, which—simply put—requires that parties to an armed conflict must at all times distinguish between civilians and combatants and between civilian objects and military objectives. While in the physical world the difference is normally readily apparent, the cyber and digital environment has added new complexities to this issue.

It is now easier than ever to involve civilians in military cyber operations and to harm them using these means. Most alarmingly, the behaviors of some parties involved in conflicts may bring about both of these consequences at the same time. To illustrate this phenomenon, consider the following three scenarios inspired by recent incidents and situations in armed conflicts:

Scenario 1: Engagement of civilians in offensive cyber operations against enemy targets. Such involvement may range from the simplest forms (such as joining a distributed denial of service attack) to more complex ones (such as cyber operations to disrupt assets or infrastructure or to exfiltrate data). The state in question may see advantages in the relatively low costs of recruiting and organizing civilians via digital means—such as social media and web fora—as well as in increasing its operational efficiency by providing tools and methods to a large group at a fast pace via websites, software repositories, or social media.

Scenario 2: Repurposing of civilian smartphone apps for military use. Existing e-government and other civilian apps may be "enhanced" during armed conflict by building in new functionalities that encourage the users to contribute to the military effort. For example, an app can ask its users to report the movements of enemy troops by uploading location-tagged images or it can provide them with information on how to attack the enemy. Given that the apps would already be well understood by the population, their use would likely not require a training period, thus allowing the new capabilities to be used almost immediately. For the state in question, an existing community of digital citizens familiar with a given app may present an opportunity to rapidly increase its offensive capabilities in time of war.

Scenario 3: Cyber defense by private civilian companies. Either voluntarily or out of a domestic legal obligation, private companies—in other words, civilian entities—that control cyber infrastructure (for example, cybersecurity companies or private security operation centers) may defend against deliberate cyberattacks originating from abroad, or they may share threat intelligence with government authorities such as national cyber defense entities. These laws may also provide for enforcement of restrictions on the use of specific digital technologies or services and thus could serve as a quasi-sanction against private companies that are based in other states. If this occurs during armed conflicts, these forms of cyber defense may thwart or impede the enemy's military cyber operations.

These three scenarios highlight different forms of civilian involvement, some of which are ostensibly voluntary and others of which may be encouraged by states or even mandated by law. What they have in common, though, is that they draw civilians into a space that is normally occupied by the military, potentially blurring the lines between civilians and combatants in cyberspace.

The Blurring Line Between Civilians and Combatants

Civilians have performed military functions during armed conflicts and assisted in war efforts since time immemorial. The digitalization of societies, however, has fundamentally shifted the role of civilian involvement in conflicts in both quality and quantity.

The main qualitative shift is that these activities are now much closer to the actual conduct of military operations: Civilian involvement has moved from the production or provision of food, shelter, or equipment at some distance from the physical battlefield to the direct contribution to the operations on the digital battlefield as support to kinetic operations.

The main quantitative shift is that, in the digital space, it is much easier to scale civilian activity in conflicts, as groups comprising thousands or even tens of thousands of individuals may be formed and coordinated online in a matter of hours. Similarly, the attack surface of societies has vastly increased. Digital devices, apps, and networks exist almost everywhere, which means that in times of armed conflict, there are exponentially more vulnerabilities than in the wars of the past.

These developments have some major implications that can be broken down roughly into four main areas:

- **Civilians as digital warriors.** Civilians may replicate everyday activities (downloading and installing an application or other kinds of software, sending messages, clicking buttons on web interface, and so on) with a purpose to actively contribute to the offensive capabilities of an armed force, for example, by installing and using an application to carry out cyberattacks. It is important to emphasize that computer interfaces (such as screens and keyboards) continue to perpetuate an illusory and artificial separation between the digital and the physical worlds, as if the former did not affect the latter.
- **Civilians as military sensors.** Civilians with digital capacities and access can often provide actionable information to armed forces, a form of information gathering known as crowdsourcing intelligence. For example, individuals with smartphones can take pictures to report and track the movements of enemy troops. Recent reports indicate that providing this sort of civilian-gathered information often has an immediate, real impact, as the information civilians send to their government could be followed by destructive military action.
- **Civilians as digital victims.** Civilian use of digital applications provided by the government can expose civilians to serious harm. For example, there have already been reports of militaries targeting civilians and their property for being suspected of using their mobile phones to report the enemy's location. If parties to armed conflicts encourage civilians to engage in this type of conduct, such incidents may become much more common, including in situations where the civilian in question was using the phone for another reason—for instance, to warn their families to leave or to seek shelter.
- **Performative nudging.** By providing these kinds of e-government-enhanced applications, states are spreading and promoting the use of these new civilian-enabled capabilities. Civilian involvement in military operations is no longer a purely voluntary act, as the general call to the population might generate. It represents what we call "performative nudging," which describes a situation in which a new online capability is made available to civilians and then is followed directly by the act for which the new function was designated—for example, stimulating the participation of civilians in armed conflicts while providing offensive digital capabilities to these civilians. This performative nudging is supported by the resilience of information and communication technology (ICT) systems. It is only through the resilience of ICT systems that states are able to push new enhanced applications and civilians are able to download and use them.

These concerns underscore the need to understand the legal constraints applicable to such forms of civilian involvement on the digital battlefield.

The Law

Under IHL, civilians are protected against attacks unless they directly participate in hostilities. This rule is articulated in Article 51(3) of Additional Protocol I and Article 13(3) of Additional Protocol II and reflects customary international law in both international and non-international armed conflicts.

Importantly, not every form of civilian involvement in war efforts qualifies as direct participation in hostilities (see paragraph 1945 of the International Committee of the Red Cross's [ICRC's] commentary on Article 51 of Additional Protocol I). While the treaty provisions cited above do not contain more precise criteria for direct participation in hostilities, the ICRC has published an interpretive guidance on this issue. According to the ICRC, an act amounts to direct participation in hostilities if it meets the following three cumulative conditions:

- 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 (known as the threshold of harm criterion).
- 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 (known as the direct causation criterion).
- 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 (known as the belligerent nexus criterion).

In our view, these criteria set the bar very high, and most forms of civilian involvement do not actually clear it. This article is not the place for a detailed legal analysis of the factual patterns identified above, but to illustrate this point, take the scenario of the repurposing of civilian smartphone apps for military use, which has received some attention thus far (see here, here, or here). In order for conduct to qualify as direct participation in hostilities, it must meet all three of the criteria—threshold of harm, direct causation, and belligerent nexus—simultaneously.

First, most forms of information provided to the military through repurposed apps would likely be too general or insignificant to meet the threshold of harm criterion. In the traditional kinetic context, there is a "general agreement that civilians merely answering questions asked by passing military personnel could not be considered as directly participating in hostilities," according to the ICRC. The same is true of digital intelligence sharing.

Second, the direct causation criterion is even more difficult to meet. To do so, the information in question would need to constitute "an integral part of a concrete and coordinated tactical operation," according to the ICRC's interpretive guidance. Unless the civilian using the app was gathering and transmitting the information as part of a coordinated operation for the purposes of a specific attack, their involvement would not clear this hurdle either.

Last, the belligerent nexus criterion presents its own challenges. Informing one party involved in a conflict about the military actions of another may be intended specifically to support one to the detriment of another, thus fulfilling the criterion. However, one may also do so in order to enable civilian warning and evacuation, support the work of civil defense organizations, or for other nonbelligerent purposes, in which case the criterion would not be met. The same would be the case if the information—for example, questions and answers about weather conditions—transmitted through an app were so general that the civilians involved would be "totally unaware of the role they are playing in the conduct of hostilities."

Only if a certain form of civilian involvement meets all three of these criteria simultaneously will their conduct qualify as direct participation in hostilities. Although our view is that this happens only exceptionally, we acknowledge that others may disagree.

Potential disagreement about whether or not civilian activity constitutes direct participation in hostilities underscores the need to understand further applicable legal safeguards for civilians. It would certainly not be correct to infer that if a civilian's involvement reached the level of direct participation in hostilities, they may automatically be targeted by the enemy forces. The applicable restrictions can be broken down roughly into four categories:

- **Territorial considerations.** If the civilian in question finds themselves outside of the territories of the parties of the conflict, other bodies of law including *jus ad bellum*, law of neutrality, and human rights law will contain numerous relevant limitations.
- **Temporal considerations.** The loss of protection is limited to the duration of each specific act amounting to direct participation in hostilities. In the example discussed above, this is the act of providing relevant information, not the fact of having that information stored in an individual's phone afterward.
- **Uncertainty considerations:** To avoid the erroneous or arbitrary targeting of civilians, parties to a conflict must take all feasible precautions when verifying whether a person is a civilian and, if that is the case, whether they are directly participating in hostilities. In any case of doubt, the person in question must be presumed to be protected against direct attack.
- **Contextual considerations:** Even if a civilian loses protection from attack, the attack is still governed by other rules of IHL. In particular, if attacking the individual was expected to result in disproportionate incidental civilian harm or if it was feasible to obtain the same military advantage while causing less or no incidental civilian harm, then attacking the individual would be prohibited by IHL.

Conclusion

Even in combination, however, these safeguards cannot prevent all negative outcomes of the involvement of civilians in military cyber and digital activities. As noted, the interpretation of the applicable law in this area is far from settled, and there are signs that some militaries might take more permissive views than those proposed in this piece. This would expose numerous civilians to grave risk of harm during armed conflict.

The ease with which offensive digital means and tools can be made available to civilians increases this exposure. The very fact that offensive capabilities are made available prompts civilians to enter the battlefield and to immediately operate with the capabilities with which they are equipped.

Furthermore, the fact that the methods and tools used on the digital battlefield are based on existing civilian functionalities facilitates their adoption and use. States may take advantage of digital civilian communities on various platforms and build their own digital weapons with the intention of quick and easy adoption and use.

Ultimately, it is up to states to prevent the osmosis between civilian and military digital tools. For example, even the integration of military functionalities within applications originally developed for civilian use is a planned and voluntary act on the part of states.

If the lines become unclear, then parties to armed conflicts may gradually begin to err on the side of considering all individuals in the enemy population as involved in hostile acts, thus diminishing existing restraints on attacks against them. Over time, this would erode the principle of distinction, with dangerous ripple effects on the interpretation of all rules of IHL that flow from it. From a broader perspective, the extent to which these practices expose civilians to the risk of grave injury or loss of life raises additional concerns under international human rights law, particularly regarding the concerned individuals' right to life (a topic that deserves more space than this article permits).

Furthermore, the distribution of offensive methods and tools to civilians in the digital domain has already changed civilian behavior during armed conflicts: from the resistance behavior of populations against enemy armed forces on the ground, to digital operations of civilians against civilians (individuals, private companies, or public civilian entities), which are located at remote distances, or even outside the areas of armed conflict, and by populations that are not even involved in the conflict. These new realities have and will continue to have a growing impact on civilian populations living in the conflict-affected territories: Digital operations against civilian infrastructures—by disrupting the delivery of services and goods or through the exfiltration of sensitive and protected data—will have economic and social consequences extending into the medium and long terms.

To avoid these challenges, states should reverse the risky trend of civilianization of the digital battlefield by reaffirming the lines that distinguish between civilians and militaries. Doing so will not only ultimately address the immediate harmful consequences of civilian involvement in armed conflicts but also prevent the negative long-term impacts that this trend may otherwise have on entire populations and societies.

Topics: Cybersecurity and Deterrence, Cybersecurity, International Law, International Law: LOAC: Distinction

Tags: International Law, civilian, Civilian Harm and Response, civilians, Distinction, Cyber & Technology

Dr. Kubo Mačák is a Legal Adviser in the Legal Division of the International Committee of the Red Cross (ICRC), assigned jointly to the Arms and Conduct of Hostilities Unit and the Commentaries Unit. Prior to joining the ICRC in 2019, he worked as an Associate Professor at the University of Exeter in the UK. Kubo is the author of the book Internationalized Armed Conflicts in International Law (Oxford University Press 2018) and of multiple articles in peer-reviewed journals including the International Review of the Red Cross, the Journal of Cyber Policy, and the Journal of Conflict and Security Law. Kubo is also the General Editor of the Cyber Law Toolkit, an interactive online resource on the international law of cyber operations.

KuboMacak

Mauro Vignati is adviser on new digital technologies of warfare at the International Committee of the Red Cross headquarters in Geneva, Switzerland. Mauro has 20 years of experience in cyber threat intelligence and cybersecurity. Before joining the ICRC, he worked for the Swiss federal police and the Swiss department of defense. He also worked for MELANI, Switzerland's first center for public-private partnership on cybersecurity for critical infrastructure, and for the National Cyber Security Centre, where he was tasked to establish the Vulnerability Management Unit.

vignus