HUMANITARIAN LAW & POLICY

8 rules for "civilian hackers" during war, and 4 obligations for states to restrain them

October 4, 2023, Analysis / Law and Conflict / New Technologies

12 mins read

Tilman Rodenhäuser
Thematic Legal Adviser, ICRC

Mauro Vignati
Adviser on new digital technologies of warfare, ICRC

As digital technology is changing how militaries conduct war, a *worrying trend* has emerged in which a growing number of civilians become involved in armed conflicts through digital means. Sitting at some distance from physical hostilities, including outside the countries at war, civilians – including hacktivists, to cyber security professionals, 'white hat', 'black hat' and 'patriotic' hackers – are conducting a range of cyber operations against their 'enemy'. Some have *described* civilians as 'first choice cyberwarriors' because the 'vast majority of expertise in cyber(defence) lies with the private (or civilian) sector'.

Examples of civilian hackers operating into the context of armed conflicts are diverse and many (see *here*, *here*, *here*). In particular in the international armed conflict between Russia and Ukraine, some groups *present* themselves as a 'worldwide IT community' with the mission to, in their words, 'help Ukraine win by crippling aggressor economies, blocking vital financial, infrastructural and government services, and tiring major taxpayers'. Others have *reportedly* 'called for and carried out disruptive – albeit temporary – attacks on hospital websites in both Ukraine and allied countries', among many other operations. With many groups active in this field, and some of them having thousands of hackers in their coordination channels and providing automated tools to their members, the civilian involvement in digital operations during armed conflict has reached unprecedented proportions.

This is not the first time that civilian hackers operate in to the context of an armed conflict, and likely not the last. In this post, we explain why this trend must be of concern to States and societies. Subsequently, we present 8 international humanitarian law-based rules that all hackers who carry out operations in the context of an armed conflict must comply with, and recall States’ responsibility to restrain them.

Civilians engaging in digital warfare – a worrying trend

The phenomenon of civilian hackers conducting cyber operations in the context of an armed conflicts is worrying for at least three reasons.

One, they cause harm to civilian populations, either by targeting civilian objects directly or damaging them incidentally. Some *experts* have considered civilian hackers and groups primarily as ‘cyber vigilantism’ and stress that their operations are technically not sophisticated and unlikely to cause significant effects. However, it is also true that civilian hackers and ‘armies’ have disrupted various civilian objects – including banks, companies, pharmacies, hospitals, railway networks and civilian government services.

Two, civilian hackers risk exposing themselves, and people close to them, to military operations. Depending on the type of operation they conduct, a party to an armed conflict may consider them as directly participating in hostilities (see cyber-specific analyses *here* and *here*). This means that the computers and digital infrastructure they use risk becoming military objectives, meaning that they are at risk of being attacked. Likewise, in the adversary’s eyes, and depending where the hacker sits, they may be attacked – by bullet, missile, or cyber operation.

Three, the more civilians take an active part in warfare, the more the line blurs between who is a civilian and who a combatant. As a result, the risk of harm to civilians grows; and *legal experts* have asked whether the principle of distinction, the centre-piece of international humanitarian law, will withhold this pressure.

8 rules for civilian hackers operating in the context of an armed conflict

Cyberspace is not a lawless space – even wars have limits.

It goes without saying that civilian hackers must respect the law of the countries they operate in. Where these national laws are lenient, not enforced, or if a civilian hacker decides to disregard them, in times of armed conflict international humanitarian law (IHL) provides a universally agreed set of rules that aim to safeguard civilians, and soldiers who are no longer able to fight, from some of the horrors of war. The most egregious violations of these rules constitute *war crimes*, which may be prosecuted nationally or *internationally*.

In the context of an armed conflict, IHL does not prohibit ‘hacking’ as such, and it does not prohibit civilians from conducting cyber operations against military assets. But it sets out elementary considerations of humanity on the protection of civilians, meaning obligations that everybody must respect when conducting operations in the context of an armed conflict, irrespective of the reasons for the conflict, whose goals are deemed legitimate, or whether an operation is conducted in offence or defense.

IHL consists of hundreds of rules – here is one word of caution and 8 rules that anyone who conducts a cyber operation in the context of an armed conflict (including non-States armed groups and civilian hackers) must be aware of and respect as a minimum. Groups or collectives should ensure that their members respect these limits.

Caution: Civilian hackers risk losing protection against cyber or physical attack and may be criminally prosecuted if they directly participate in hostilities through cyber means

Under IHL, civilians must not be attacked unless and for such time as they directly participate in hostilities. Conducting cyber attacks against military or civilian targets can amount to such direct ‘participation in hostilities’ and risks making civilian hackers liable to attacks. In addition, while members of a State’s armed forces (including cyber operators) enjoy impunity for lawful acts of war (such as attacking a military installation) and become ‘prisoners of war’ when captured, civilian hackers do not (*here*, para. 3634 on article 85 GCIII). If captured, they risk being considered criminals or ‘terrorists’ and prosecuted as such.

1. Do not direct cyber attacks* against civilian objects.

Civilian objects are all objects that are not military objectives. This includes civilian infrastructure, public services, companies, private property, and arguably civilian data. Military objectives do not enjoy the same protection. ‘Military objectives’ comprise primarily the physical and digital infrastructure of the military of a warring party. It may also include civilian objects, depending on whether and how they are being used by the military.

2. Do not use malware or other tools or techniques that spread automatically and damage military objectives and civilian objects indiscriminately.

For example, malware that spreads automatically, spills-over, and damages military objectives and civilian objects without distinction must not be used.

3. When planning a cyber attack against a military objective, do everything feasible to avoid or minimize the effects your operation may have on civilians.

For example, if you aim to disrupt electricity or railway services used by military forces, you must avoid or minimize the effects your operation may have on civilians. It is essential to research and understand the effects of an operation – including unintended ones – before conducting it. When planning a

cyber attack against a military objective, do everything feasible to avoid or minimize the effects your operation may have on civilians, and stop the attack if the harm to civilians risks being excessive. If you have gained access to an operating system but you do not understand the possible consequences of your operation, or realize that the harm to civilians risks being excessive, stop the attack.

4. Do not conduct any cyber operation against medical and humanitarian facilities.

Hospitals or humanitarian relief organizations must never be targeted.

5. Do not conduct any cyber attack against objects indispensable to the survival of the population or that can release dangerous forces.

In international humanitarian law, objects containing dangerous forces are defined as ‘dams, dykes and nuclear electrical generating stations’; in reality, however, chemical and similar plants also contain dangerous forces. Objects indispensable for the survival of the civilian population include, among others, drinking water installations or irrigation systems.

6. Do not make threats of violence to spread terror among the civilian population.

For example, hacking into communication systems to publish information designed primarily to spread terror among civilian populations is prohibited. Likewise, designing and spreading graphic content to spread terror among civilians in order to make them flee is unlawful.

7. Do not incite violations of international humanitarian law.

Do not encourage or enable others to conduct cyber or other operations against civilians or civilian objects. For example, do not share technical details in communication channels to facilitate attacks against civilian institutions.

8. Comply with these rules even if the enemy does not.

Revenge or reciprocity are no excuses for violations of international humanitarian law.

* Under IHL, and in the context of cyber operations, the *notion of attack* refers to cyber operations that can be reasonably expected to result – directly or indirectly – in damage, disabling, or destruction of objects (such as infrastructure and, arguably, data) or injury or death of people. It does not, for instance, include cyber operations aimed at obtaining unauthorized access to information.

For more detailed positions of the International Committee of the Red Cross on IHL and cyber operations, see *here* and *here*. To learn more about how international law applies in cyberspace, consult the ‘*Cyberlaw Toolkit*’.

Hackers do not live in cyberspace – States must impose limits

States should not encourage or tolerate civilian hackers conducting cyber operations in to the context of an armed conflict.

The more civilian hackers engage in cyber operations, the greater the risk of operations that violate applicable law and blur the line between combatants and civilians. Therefore, the ICRC has called on States to ‘*give due consideration to the risk of exposing civilians to harm if encouraging or requiring them to be involved in military cyber operations*’.

From a legal point of view, all States have pledged to not ‘knowingly allow their territory to be used for internationally wrongful acts using ICTs’ (*here*, para. 13(c)). While formulated as a political commitment, this norm reflects States’ ‘due diligence’ obligation under international law, including in respect of civilian hackers operating from their territory (see *here*). Any State that is committed to the rule of law or a ‘rules-based international order’ must not close its eyes when people on its territory conduct cyber operations in disregard of national or international law, even if directed against an adversary.

This means, first and foremost, to adopt and enforce national laws that regulate civilian hacking.

In addition, and specifically with regard to the conduct of private individuals in times of armed conflict, States have undertaken to respect and to ensure respect for IHL. This legal commitment means at least four things:

First, if civilian hackers act under the instruction, direction or control of a State, that State is internationally legally responsible for any conduct of those individuals that is inconsistent with the State’s international legal obligations, including international humanitarian law (see *here*, article 8, and *here*). For instance, if a State uses private individuals or groups as “volunteers” and instructs them to carry out particular cyber operations in disregard of international law, the state is legally responsible for such violations (see *here*, para. 2 on article 8). (This responsibility comes in addition to possible criminal responsibility of the private hacker).

Second, States must not encourage civilians or groups to act in violation of international humanitarian law (see *here*, para. 220). Concretely, this means that State agents – be they military, intelligence, or any other government actor – are prohibited from encouraging civilians or groups to, for example, direct cyber attacks against civilian objects, irrespective of which channel or app is used to do so.

Third, States have a due diligence obligation to prevent international humanitarian law violations by civilian hackers on their territory (see *here*, para. 183). Of course, a State cannot prevent all violations of the law. However, it must take feasible measures, such as taking *public positions* requiring civilian hackers not to conduct cyber operations in relation to armed conflicts, to respect IHL if they do, and suppress violations under national law (see next).

Fourth, States have an obligation to prosecute war crimes and take measures necessary to suppress other IHL violations (article *49/50/129/146* GCI-IV; article *85* Additional Protocol I). First, this requires the adoption and enforcement of the necessary laws that criminalize cyber operations amounting to war crimes, and second, to take effective measures to stop all other violations of IHL, which may include legal, disciplinary, or administrative measures. Clearly, adopting laws or policies that turn a blind eye on civilian hackers conducting cyber operations as long as these operations are committed against ‘the enemy’ does not comply with this obligation.

***

IHL sets out essential rules to limit the effects of armed conflicts on civilians. No one that participates in war is beyond these rules. In particular, every hacker that conducts operations in the context of an armed conflict must respect them, and States must ensure this is the case to protect civilian populations against harm.

Editor’s note: This article was originally published in EJIL:Talk! and is available *here*.

See also

- March 7, 2023, *Towards common understandings: the application of established IHL principles to cyber operations*, Kubo Mačák & Tilman Rodenhäuser
- Pete Renals, *Future developments in military cyber operations and their impact on the risk of civilian harm*, June 24, 2021
- Ellie Shami, *Assessing the risks of civilian harm from military cyber operations during armed conflicts*, June 22, 2021
- Noëlle van der Waag-Cowling, *Stepping into the breach: military responses to global cyber insecurity*, June 17, 2021
- Kubo Mačák & Ewan Lawson, *Avoiding civilian harm during military cyber operations: six key takeaways*, June 15, 2021

Tags: civilian hackers, cyber technology, cyber warfare, digital technology, digital warfare, Geneva Conventions

You may also be interested in:

Armed conflict in Sudan: a recap of the basic IHL rules applicable in non-international armed conflicts

15 mins read

Analysis / Law and Conflict / New Technologies Julie Lefolle & Jelena Nikolic

On 15 April 2023, the world watched the eruption of hostilities in Khartoum, the capital of Sudan, which also spread to other parts ...

A safety net for prisoners of war: five key principles of the Third Geneva Convention

11 mins read

Analysis / Law and Conflict / New Technologies Yvette Issar

After the Second World War, countries came together to improve the legal protection available to certain categories of persons – including prisoners of ...