NR. 624 E
15.06.2022

STEPHAN KOLOSSA
PhD Student
IFHV
Ruhr-Universität Bochum

QUESTIONS
Stephan.kolossa@rub.de

Völkerrechtsblog
INTERNATIONAL LAW & INTERNATIONAL LEGAL THOUGHT

IFHV

BOFAXE

The Dangers of Hacktivism (Part 1)

HOW CYBER OPERATIONS BY PRIVATE INDIVIDUALS MAY AMOUNT TO WARFARE

The Russian Federation (Russia) has turned almost the whole Western world against it by attacking and invading Ukraine. While States are intensively debating about the strictest yet legally sound ways to react to Russia's aggression, private individuals have already started to engage more actively in the fight against Russia, partially as soldiers joining the armed forces on the ground, yet even more frequently online by using their computers and hacking skills. In fact, Ukraine's Deputy Prime Minister Mykhailo Fedorov officially called for capable talents to join the Ukrainian IT army. Irrespective of how many actually join the IT army, this contribution seeks to address the question whether and how private individuals can become an actual part of the conflict.

Activist groups of hackers (also known as "hacktivists") by now have taken a very active role in the conflict. A case in point is the international activist collective "Anonymous", which has explicitly declared "cyber war" against Russia. Hacks have been targeting Russian media, internet providers, and intergovernmental websites. Anonymous claimed responsibility for numerous cyber incidents involving distributed denial of service (DDoS) attacks, hacking into various databases of the Russian government, and other cyber operations. In their video on Twitter, Anonymous announced that "[s]oon you will feel the full wrath of the world's hackers." Other groups such as "Squad 303" or "NB65" have joined efforts as well, just as one of the members of Squad 303 declared: "We work together with Anonymous all the time and I now consider myself a member of the Anonymous movement" claiming to be "on the barricade with a rifle during the day and hacking with the Squad/Anonymous at night". Therefore, the question arises: Is it possible for hacktivists to directly participate in the armed conflict in a way which would allow Russia to strike back and ultimately kill them?

How Civilian Can Hacktivists Be?

The conduct of cyber operations needs to be measured against international humanitarian law, just as the International Committee of the Red Cross (ICRC) has recently argued in a statement delivered at the United Nations Open-Ended Working Group on security of and in the use of information and communications technologies (OEWG). It is undisputed that the ongoing conflict between Russia and Ukraine, as an armed conflict amongst two sovereign states, is an international conflict under international humanitarian law. However, hacktivists and in particular the scattered group of hacktivists operating under the caption "Anonymous" are known to be an anarchist group operating neither as part of the armed forces of Ukraine, Russia nor any other sovereign state. In fact it is most likely that this group does not even possess a strict hierarchical structure but forms a rather decentralized, yet like-minded collective. It is therefore difficult to argue that they represent an organized armed group that engages in their own separate non-international armed conflict against Russia besides the ongoing international armed conflict. For the same reason, they do not represent any kind of "irregular" armed forces, neither are they part of the regular Ukrainian military as they have not subjected themselves to their command. Just as one hacktivist put it:

"We [...] dedicate our time outside of jobs and familial obligations to this [...] We ask nothing in return. It's just the right thing to do."

Article 51(2) First Additional Protocol to the Geneva Conventions (AP I) states that "[t]he civilian population as such, as well as individual civilians, shall not be the object of attack." Private hacktivists therefore generally do not become involved in the conflict under international humanitarian law. Article 51(3) AP I, however, adds that civilians only enjoy protection "unless and for such time as they take a direct part in hostilities." The decisive question to answer is: Are hacktivists civilians directly participating in the ongoing hostilities between Russia and Ukraine? The protection of civilians and the principle of distinction are fundamental parts of international humanitarian law and have been accepted even by States not party to AP I. The Supreme Court of Israel, inter alia stated in its decision on targeted killings that "all of the parts of article 51(3) of The First Protocol express customary international law" (para. 30 and in a slightly different wording para. 38). Unfortunately, there is still no uniform consensus on the exact meaning of direct participation in hostilities. Besides the various contentious aspects (e.g. the duration of the participation in hostilities) the main issue remains whether it is generally possible to participate in a conflict as a hacktivist by conducting cyber operations.

VERANTWORTUNG Die BOFAXE werden vom Institut für Friedenssicherungsrecht und Humanitäres Völkerrecht der Ruhr-Universität Bochum herausgegeben: IFHV, Massenbergstrasse 9b, 44787 Bochum, Tel.: +49 (0)234/32-27366, Fax: +49 (0)234/32-14208, Web: http://www.ruhr-uni-bochum.de/ifhv/. Bei Interesse am Bezug der BOFAXE wenden Sie sich bitte an: ifhv-publications@rub.de. **FÜR DEN INHALT IST DER JEWEILIGE VERFASSER ALLEIN VERANTWORTLICH.**

NR. 624 E
15.06.2022

STEPHAN KOLOSSA
PhD Student
IFHV
Ruhr-Universität Bochum

QUESTIONS
Stephan.kolossa@rub.de

Völkerrechtsblog
INTERNATIONAL LAW & INTERNATIONAL LEGAL THOUGHT

IFHV

BOFAXE

The Dangers of Hacktivism (Part 2)

HOW CYBER OPERATIONS BY PRIVATE INDIVIDUALS MAY AMOUNT TO WARFARE

The most thorough work on this notion has most likely been done by the ICRC in its "Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law" (hereinafter referred to as "ICRC Guidance"). The ICRC Guidance was the result of a study the ICRC commissioned in 2009 in which it examined what qualifies as direct participation under customary international humanitarian law. The findings are not binding but for the purpose of this analysis persuasive in the determination of what direct participation is. According to the ICRC Guidance, in order to become a legally relevant act under humanitarian law, the cyber operations must first reach a certain threshold of harm, they must secondly directly cause that harm, and they must thirdly be designed to support one party of the conflict over the other (a criterion also known as belligerent nexus) (ICRC Guidance, pp. 46 et seq.). The fact that the hacktivists' cyber operations against the Russian government are a direct reaction to the ongoing war and that they are meant to disadvantage the Russian over the Ukrainian side is not doubted. The decisive question is whether the operations meet the necessary threshold. Whether or not a hacktivist is considered to participate in the ongoing conflict does not refer to his or her status, function or affiliation, but to his or her engagement in specific hostile acts (ICRC Guidance, p. 44). It does not matter, if hacktivists act spontaneously, sporadic, or on an unorganized basis, as long as the specific operation meets the necessary threshold of harm. Thus, is hacking the Russian Central Bank or disrupting Russian IT infrastructure through DDoS attacks an act of war – or are the hacktivists nothing else than ordinary criminals?

Cyber Hacktivism on the Edge of Direct Participation in Hostilities

According to the ICRC Guidance the specific 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" (ICRC Guidance, pp. 46 et seq.). It is enough for the cyber operation in question to likely produce harm for the named targets, it does not have to actually result in material harm. The likelihood of harm is a matter of fact.

When targeting the military, it is sufficient to sabotage military activities or to disturb deployments of troops. The threshold is lower than in the context of civilian targets. At the same time "the interruption of electricity, water, or food supplies, [...] the manipulation of computer networks, [...] would not, in the absence of adverse military effects, cause the kind and degree of harm required to qualify as direct participation in hostilities." (ICRC Guidance, p. 50). Yet for hacktivists, it means that it is not enough to hack any kind of government database or specifically the Russian Central Bank. The target must have a military function. Hence, if the reports claiming that a group of cyber warriors hacked servers of a railway company and blocked nearly 200 trains that were meant to carry Russian troops and equipment for a deployment in Ukraine were true, this would amount to direct participation. An act of such dimension is however only mentioned in Belarusian news and not confirmed by other sources, which is why it is difficult to assess whether it has actually happened. According to other media reports (e.g. here and here), however, Anonymous has released personal data of 120,000 Russian soldiers. The data included names, dates of birth, addresses, unit affiliation, and passport numbers. The public revealing of private personal information (also referred to as "doxing") was meant to facilitate future investigations for war crimes or proceedings before war crime tribunals, in light of mass atrocities that happened particularly in Bucha. Even if doxing members of the military was meant to intimidate the respective soldiers as they would potentially face charges for war crimes, such actions are not likely to cause an adverse effect on the military. The Russian maneuvers are no secret mission where revealing the soldiers' identities would put the mission at risk. Moreover, the Russian point of view is that leading the conflict in Ukraine is legal. If this is their stance, they naturally do not fear being prosecuted for war crimes. Publishing personal information about soldiers as such does not impede a concrete military action or strategy, nor is it likely to. Hence, since the crucial aspect is the probability of an adverse military effect, Russian troops are not affected in their operations.

Considering civilian targets of the hacktivism, civilian persons appear not likely to having been injured or killed by the cyber operations. Hacking and encrypting servers and databases are, however, likely to affect civilian data on a largescale basis. This shifts the question and the focus to whether civilian data may be deemed as objects under the mentioned definition of the threshold of harm. Indeed, current developments point to this outcome. France, for example, in its latest statement on the "Droit international appliqué aux operations dans le cyberspace" (pp. 15 et seq.) considers personal data of civilians a potential object. Chile has emphasized that "an attack directed exclusively at computer data could well produce adverse consequences affecting the civilian population" (para. 48). This may be the case when a state's social security database is encrypted, and the corresponding personal data is destroyed. While not clearly interpreting data as an object in this context, Guyana highlighted that "the deletion, suppression, corruption of data may have far reaching consequences" (para. 48). Accordingly, civilian data is not only a proxy for targeting civilians but can also be subject of hacks as an object in and of itself. This question of whether data is an object will gain tremendous relevance in the future.

The hacktivist cyber operations in the context of the ongoing conflict between Russia and Ukraine show that they oftentimes come close to a direct participation in the hostilities. So far, the hacktivists seem to have remained below the threshold. Particularly the current developments considering civilian data as objects show that private cyber operations are not per se irrelevant under international humanitarian law, but may very well amount to a serious engagement with the ongoing conflict. Although some say that "hacktivism is one of the most accessible forms of striking at an unjust regime or its supporting infrastructure", beyond a certain threshold it bears the risk of becoming more directly involved in the conflict than one would wish.

VERANTWORTUNG Die BOFAXE werden vom Institut für Friedenssicherungsrecht und Humanitäres Völkerrecht der Ruhr-Universität Bochum herausgegeben: IFHV, Massenbergstrasse 9b, 44787 Bochum, Tel.: +49 (0)234/32-27366, Fax: +49 (0)234/32-14208, Web: http://www.ruhr-uni-bochum.de/ifhv/. Bei Interesse am Bezug der BOFAXE wenden Sie sich bitte an: ifhv-publications@rub.de. **FÜR DEN INHALT IST DER JEWEILIGE VERFASSER ALLEIN VERANTWORTLICH.**