Nr. 484E
26.02.2016

BOFAXE

Targeting Hackers AFK
Civilian IT-Experts as Targets in Non-International Armed Conflicts

Autor / Nachfragen

Simon Gauseweg
Europa-Universität Viadrina, Frankfurt (Oder)

Nachfragen:
euv92030@europa-uni.de

Webseite

http://www.ifhv.de

Fokus

An alledged ISIL-'hacker' was killed in a U.S. drone strike in december. Targeting (civilian) hackers 'AFK' is only possible if they are *members* of the group of fighting non-state actors – or qualify as civilians taking *direct participation in hostilities* and thus lose their protection. The killed hacker allegedly conducted 'hacking efforts', 'anti-surveillance technology' and 'weapons development' – all of which not necessarily qualifies for *dph*. He was said, however, to be one of ISIL's leaders.

Quellen
http://www.centcom.mil/en/news/articles/coalition-killed-10-senior-isil-leaders-in-december
Melzer, Interpretive Guidance on the Notion of Direct Participation in Hostilities, Geneva 2009

According to the U.S. Central Command (CENTCOM), an IT-expert allegedly associated with the terror-militia "Islamic State of Iraq and the Levant" (ISIL) was killed in a drone strike on December 10, 2015 near Raqqah in Syria. The Bangladeshi had learned his craft in the United Kingdom and „supported ISIL hacking efforts, anti-surveillance technology and weapons development," CENTCOM reported on December 29. As stated in newspapers, he had replaced ISIL's "chief hacker" who was killed in August 2015. While it is possible that the information-technician in question also actively engaged in hostilities or pulled the strings on (suicide) attacks, CENTCOM seem to have targeted him "away from (his) keyboard" (AFK). The present BOFAX addresses the question whether this targeting was legal under international humanitarian law. Firstly, it has to be assessed that the applicable ruleset of *ius in bello* is that of the non-international armed conflict with ISIL remaining a non-state party to the conflict. Neither Syria nor the U.S. are State party to the Additional Protocol II (APII) to the Geneva Conventions (GCs). Thus, only common art. 3 GC is applicable in this context.

The U.S. called the deceased IT-expert a 'leader', implying not only membership but also (at least a minimum of) control over (at least parts of) ISIL forces. This would have rendered him a legitimate target under AP II (as a member of the organized armed group who, comparable to combatants in an international armed conflict, are always lawful military targets). This argumentation can be transferred to a conflict governed by common art. 3 GC, although rather in concept than in term. However, there is no uncontested concept of *membership* in such a non-state armed group. If the 'hacker' killed had not been a 'leader' of ISIL, a more functional approach in targeting than resorting to a hard-to-prove membership would be appreciated. And indeed both common art. 3 GC and the AP II provide a (very similar if not the same) concept to solve this problem: the direct participation in hostilities (dph).

A civilian loses protection from attack when he takes 'active' (common art. 3 GC) or 'direct' (AP II) participation in hostilities. According to an interpretive guidance of an ICRC-hosted group of experts that was eventually published by the ICRC in 2009, an act qualifies as 'dph' if it meets a certain *threshold of harm* with *direct causation* and has an *belligerent nexus*. "In order to reach the required threshold (…), a specific act must be likely to adversely affect the (…) operations or (…) capacity of a party (…) or (…) to inflict death, injury, or destruction (…)". Direct causation requires "a direct causal link between a specific act and the harm likely to result (…)". The belligerent nexus, eventually, requires that "an act must be specifically designed to directly cause the (…) harm in support of a party to the conflict and to the detriment of another" (Melzer).

Developing and/or running 'anti-surveillance technology' only reaches the required threshold, if the acts contain elements actively affecting enemy systems. Pure means of escaping (or helping to escape) U.S. or other surveillance efforts are insufficient and do not lead to loss of protection for civilians. 'Weapons development', if one wants to qualify a piece of code as a 'weapon', is most likely to fail the criterion of *direct causation*; it may, however, pass, if the software in question is directly 'tailored to the task' and its development "constitutes an integral part" of a "coordinated military operation". 'Hacking efforts' may be the most probable cause for 'hackers' losing their protection – if all three above-mentioned criteria are reached. But even then a 'hacker' loses protection only for such time the hack is actively conducted. Thus, killing the hacker in between keystrokes would be legal – targeting him AFK not. This, however, leads to the so-called revolving door problem of 'farmers by day, fighters by night': Hackers, probably 99% occupied with non-aggressive programming, can still 'raise hell' in the remaining 1% – but may only at that exact time be targeted. The concept of establishing a 'continuous combat function' (Melzer) of the civilian is used to expand the targeting options and prevent constant relapse into protection. However, the concept itself is not uncontroversial and can therefore not be generally presumed.

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.