NR. 526 E
23.05.2019

DR. IUR. TASSILO SINGER
Rechtsreferendar; vormals Wissenschaftlicher Mitarbeiter der Europa Universität Viadrina und der Universität Passau.

NACHFRAGEN:
tassilo.singer@gmx.de

Völkerrechtsblog
INTERNATIONAL LAW & INTERNATIONAL LEGAL THOUGHT

IFHV

BOFAXE

Retaliatory Strikes as a Reaction to Cyber-Attacks? (Part 2)

The recent Israeli Airstrike against HamasCyberHQ from an IHL perspective

If Hamas is seen as the government of a State, members of its armed groups are considered combatants. If seen as an OAG, armed members become lawful targets due to their continuous combat function, see Art. 51 (3) AP I. Hamas members who do not carry out a combat function – the organization has political components, too – can be classified as civilians. However, given the organization's (para) military background, it is hard to distinguish political members from members of armed groups. When a person originally classified as civilian takes up arms, it becomes a lawful target according to Art. 51 (3) AP I. *De minimis* members with military or semi-military function are lawful targets either under Art. 43 (2), 48 AP I or under Art. 51 (3) AP I. The status of Hamas members raises problems and discussions concerning the criteria and thresholds of the DPH rule. What about persons who fulfill supply, governance or executive functions? The fine line between lawful targets and protected civilians is blurred on various occasions.

To the extent known, the object of the airstrike was located in a civilian area. If the nature or purpose of the object does not make an effective contribution to military action, it shall be presumed to be used for civilian purposes as a rule of doubt (Art.52 (2), (3) AP I). Therefore, the nature and purpose of the HamasCyberHQ is decisive for the lawfulness of the strike. This depends on the actual contribution to military action and, thus, on the purpose and function of the personnel residing there. In addition, the functions and activities of the personnel determine their legal status. Provided the building was a base for the intelligence branch and the HamasCyberHQ, their functions must have contributed to the military activities. The intelligence branch regularly serves not only internal purposes but external, cross-border purposes. In view of the ongoing conflict with regular armed clashes with Israel, it is highly likely that it includes a military component. The military intelligence branch gains military advantage for Hamas when intelligence is gathered about Israel. Due to this function it becomes a military object. Therefore, an attack against the intelligence service offers a military advantage and is lawful, see Art. 51, 52 AP I.

Concerning cyber operations, the capability and functions of the cyber operatives have to be analyzed. If they conduct harmful cyber operations which can cause physical effects and destruction, especially if they can affect Israeli military operations, they do not have to be treated different than regular participants in armed operations. An example might be a cyber operation that interferes with military communication of the opponent. Persons linked to an OAG, who are able to affect military operations of another conflict party, execute military functions. Cyber operatives tasked accordingly, have to be classified likewise. If affiliated with an OAG, they have a continuous combat function. If they are not member or part of an OAG and perform their operations as civilians, they still directly participate in hostilities. It does not matter whether the personnel in question solely works on a computer in distance to the '*real*' fighting, as long as they contribute to the military efforts of a conflict party. Type, function and (intended or possible) effects of the cyber operation become decisive for the legal status.

As cyber operations can have various functions and often are 'dual-use' the distinction becomes more problematic. Many grey zones or at least close single cases arise as a 'civilian' DDOS attack (= Distributed Denial of Service Attack) can have an effect on a military operation. Thus, the lowest threshold with view to LOAC and in connection to the ongoing armed conflict has to be identified: any cyber operation that fosters the military operation, helps it to be more effective and consequently provides a military advantage. The cyber operation has to be compared to conventional operations and non-sufficient support operations. *Inter alia* DDOS attacks, the infiltration of military or governmental networks and computers with military (guidance) connection, the change of military or governmental data and the interference with signals can be qualified as a military advantage towards the other party. Besides information operations like publishing or otherwise spreading misleading information for enemy forces create military gain. Also a misinformation about the military status of a civilian object, which additionally leads to an abuse of the civilian protection status, constitutes another violation of Art. 51 AP I.

Concluding, the lawfulness of the attack depends on the single facts of the case and thereby on the type of the conducted cyber operation(s). In the case that the cyber operatives have or had conducted a cyber operation against Israel as claimed by the IDF, it is not farfetched that it was intended to create relevant military gain for Hamas. An Israeli attack against the cyber operatives therefore would have been lawful with view to the status of the HamasCyberHQ. Nevertheless, this can only be conclusively determined if some 'hard' facts of the cyber operation are published. The same is true for legal requirements like the proportionality rule and the duty to precautions. That said, the open statement on a cyber operation against Israel, its defense by the IDF and the conventional airstrike on the HamasCyberHQ present a variety of legal issues from an LOAC perspective. Although most of them derive from existing legal discussions about the content and interpretation of LOAC, the peculiarities of the conduct of cyber operations, their functions and their effects lead to new grey zones. There is thus an urgent need for further clarification by States on their interpretation and categorization of 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.