Nr. 463E
16.01.2015

BOFAXE

Skirmishes in cyber space and the notion of 'attack' under international law

Autor / Nachfragen

Tilman Rodenhäuser
PhD Candidate
Graduate Institute, Geneva

Nachfragen:
Tilman.rodenhauser@iheid.ch

Webseite

http://www.ifhv.de

Fokus

Kurztext:
In light of recent skirmishes in cyber space, this Bofax discusses whether and to what extent the notion of 'armed attack' under *ius ad bellum* and 'attack' under *ius in bello* may apply to cyber operations that do not cause any death or physical destruction.

Quellen:
Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, 2013.

Cordula Dröge, *Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians*, IRRC, No. 886, 2012.

As the year 2014 approached its end, a number of 'cyber attacks' made headlines. Most prominent among them was the allegedly North Korean attack against Sony Pictures. While receiving less attention in international media, just before Christmas North Korea became itself victim of what insiders think was a 'distributed denial of service' attack (DDoS). Such an operation overloads the victim's servers with data-intake, which temporarily blocks the servers without, however, causing lasting damage. In the case of North Korea, the attack 'switched off' the admittedly underdeveloped and easy to manipulate Internet of the entire country for more than 9 hours. While colloquially referred to as 'attacks', it is controversial whether an operation such as the one against North Korea may also constitute an 'attack' as legally defined in *ius ad bellum* and *ius in bello*. These two aspects are discussed in the following.

First, considered from an *ius ad bellum* perspective, could a DDoS amount to an 'armed attack' as set out in article 51 UNC permitting the attacked state to resort to force in self-defence? While the term 'armed attack' is generally undefined under international treaty law, in the Nicaragua judgment the ICJ suggested that in order to constitute an armed attack, particularly the 'scale and effects' of an attack should be considered (para. 195). It is rather uncontroversial to state that cyber operations causing death, injury or physical destruction can meet the threshold. In contrast, in the Tallinn Manual government experts stated that operations, like a DDoS, that are 'highly invasive' but 'cause only inconvenience' may not qualify as an armed attack. According to the limited information available on the actual effects in North Korea, this is probably what happened. However, if such an attack is committed against a technologically advanced state causing severe consequences such as the interruption of stock trade at some of the world's main stock markets, the classification of the situation could potentially change. As experts cautioned in the Tallinn Manual: 'some may categorize massive cyber operations that cripple an economy as a use of force even though economic coercion is presumptively lawful'.

A related but distinct question is whether such an attack could trigger an international or non-international armed conflict (see the very insightful discussion by Dröge).

Second, let us assume that a 'denial of service attack' occurs in the context of an armed conflict. Would a DDoS constitute an 'attack' regulated by the rules on the conduct of hostilities under IHL? If this was the case, the attacker would have to respect at least the fundamental principles of distinction, proportionality, and precautions, each of which raise controversial debates on their application in cyber space. Art. 49 API defines 'attacks' as 'acts of violence against the adversary, whether in offence or in defence'. The Tallinn Manual states convincingly that attacks under IHL include not only kinetic but also non-kinetic operations if the latter can be 'reasonably expected to cause injury or death to persons or damage or destruction to objects'. Yet, this may not be the case if an operation only affects the functionality of an object or service. Dörrmann advanced an interesting argument that would broaden the scope of attacks under IHL to some extent. Invoking a contextual understanding of the notion of 'attack' under IHL, he suggested: 'Given that elsewhere in the same section of AP I, namely in the definition of a military objective, reference is made to neutralization of an object as a possible result of an attack, one may conclude that the mere disabling of an object … without destroying it should be qualified as an attack as well.' While government experts involved in the Tallinn Manual process did not agree on this point, it emphasizes that in order to respond to new challenges posed by cyber operations legal experts have to present innovative solutions, especially in order to adapt the protective scope of IHL.

As numerous states work intensely on their cyber security capabilities (see, f.e., ARD documentary 'Schlachtfeld Internet'), recent skirmishes in cyber space reemphasize that it is similarly important to engage in dialogue and come to agreement on how existing regulations may respond to new challenges. Conflicting interpretations of what constitutes an 'attack' under different fields of international law bear great risks for escalating tensions in international relations.

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/. Die BOFAXE werden vom Deutschen Roten Kreuz unterstützt. Bei Interesse am Bezug der BOFAXE wenden Sie sich bitte an: ifhv-publications@rub.de.