Nr. 478E
01.10.2015
BOFAXE

A First Cyber Arms Control Accord?
A (Planned) Agreement between the U.S. and China under Scrutiny

Autor / Nachfragen

Simon Gauseweg
Europa-Universität Viadrina, Frankfurt (Oder)

Nachfragen:
euv92030@europa-uni.de

Webseite

http://www.ifhv.de

Fokus

It is grossly exaggerated to call the allegedly planned agreement between the USA and PRC an "arms control accord". The definition of methods of 'cyber warfare' as 'weapons' is at least problematic. Furthermore, the agreement will not restrict the States' use of 'cyber'-means during wartime. Referring to 'critical infrastructure', the agreement nothing but reflects already existent law, stressing only that neither State planned to break it *first*.

Quelle
David E. Sanger, U.S. and China Seek Arms Deal for Cyberspace, *The New York Times*, 19.09.2015, nytimes.com

The *New York Times* called it something that "could become the **first arms control accord** for cyberspace" when it disclosed some information about a bilateral agreement between the United States of America and the People's Republic of China. The agreement was allegedly to be officially announced during the Chinese president's state visit in late september. Referring to officials involved in the talks, the *Times* reported this agreement embraced "a commitment by each country that it [would] not be the first to use cyberweapons to cripple the other's critical infrastructure during peacetime." But neither a text of an agreement was published, nor an official statement heard. Still, the mere news of such an agreement raises curiosity – and scrutiny: First, to qualify for the 'arms control'-label, the agreement would have to contain a definition of the objects to be controlled, meaning 'cyber weapons'. This item alone leaves room for elaborate discussion, provided the authors are willing to go farther than the assumption that every means or method of IT capable to cause damage qualified for a 'cyber weapon' (cf. Rule 41 of the Tallinn Manual). But even if there was a definition that on the one hand was broad enough for a practical application of the agreement but would not, on the other hand, encompass virtually every piece of standard-software, traditional arms control accords apply both in times of peace and of war: While during peace-time the production and proliferation are limited (or, at best, prohibited), States also would refrain from using the respective weapons in war-time. According to the alleged U.S. and Chinese plans, the agreement will remain silent on limitations of the use of 'cyber capabilities' during armed conflict. Even more, according to the quoted "officials involved in the talks", the agreement will not go further than the concept of 'first-use-doctrine' applied to cyber-warfare, so that Retaliatory strikes will not be governed by the arrangement.

Furthermore, the agreement aims at barring the "crippling of critical infrastructure" by means of cyber-warfare. The *New York Times* refers to examples like "power stations, banking systems, cellphone-networks and hospitals". When talking about "arms control" and "arms use", i.e. the **law of armed conflict**, these examples are at the brink of uselessness. The most blatant case is the hospital: Already the Hague Regulations of 1907 prohibit attacks on hospitals (Art. 28). Those attacks would in most cases be considered a war crime. Regarding power stations, Art. 56 of the Additional Protocol I (1971) to the Geneva Conventions (AP I) has to be recognized, prohibiting in essence the destruction of a certain amount of power plants (namely in dams and nuclear-powered facilities). But even taking the example of a wind farm, banking systems or communications networks that are not crucial for the civilian population's survival (cf. Art. 54 AP I), one can still argue that they do not constitute military objectives, but civilian objects (Art. 48, 52 AP I) – or that an attack on these objects would actually constitute an attack on the civilian population itself (Art. 51 (1), (2) AP I) and would thus be forbidden. It has to be recognized that the term 'critical infrastructure' includes the assessment 'critical' for a reason. In most cases, these breaches would also constitute war-crimes under the Statute of the ICC. And this is all ius in bello, the international law's 'emergency rules' for when the prohibition on the use of force (Art. 2 (4) UNCh) failed to work. As a rule of thumb, one can deem anything that would constitute a war crime under the law of armed conflict forbidden *a fortiori* in peace time. Also, the first strike in an armed conflict that changes the applicable body of law from peace-law to the law of armed conflict, has to adhere to the basic principle of distinction of which the cited articles of AP I derive. Summing up, it can be stated that attacks on 'critical infrastructure' are already at least problematic under today's law. Any agreement aiming at a prohibition of those attacks would just re-state the signatories' will to adhere to existing law. This is neither new, nor a real improvement.

Verantwortung

Die BOFAXE werden vom Institut für Friedenssicherungsrecht und Humanitäres Völkerrecht der Ruhr-Universität Bochum herausgegeben: IFHV, Massenbergstrasse 9b, Ruhr-Universität Bochum, 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.