Nr. 462D
06.01.2015

BOFAXE

Hacking als Kriegsgrund?
Cyber-Spionage, Völkerrecht und das *ius ad bellum*

Autor / Nachfragen

Simon Gauseweg
Europa-Universität Viadrina, Frankfurt (Oder)

Nachfragen:
euv92030@europa-uni.de

Webseite

http://www.ifhv.de

Fokus

Sog. "Cyber-Spionage" gegen die Bundesrepublik Deutschland nimmt zu. Obgleich keine Norm des internationalen Recht Spionage ausdrücklich gestattet, ist sie nicht im Umkehrschluss verboten. Die Eigenheiten der Cyberspionage bewirken allerdings eine Verletzung der territorialen Souveränität des Zielstaates.

Quellen:
Katharina Ziolkowski, Peacetime Cyber Espionage – New Tendencies in Public International Law, in: Peacetime Regime for State Activities in Cyberspace 2013.
Tallinn Manual on the International Humanitarian Law Applicable to Cyberwarfare 2013.

Drei- bis fünfmal am Tag greifen staatliche Akteure Computersysteme der deutschen Regierung an, berichten die Präsidenten der Bundesamtes für Sicherheit in der Informationstechnik (BSI) und des Verfassungsschutzes. Letzterer bezeichnete kürzlich Berlin als „Hauptstadt der Cyber-Spionage". Unterdessen brachte der Konzern Sony kürzlich einen Film nicht in die Kinos, da er angeblich vom Geheimdienst Nordkoreas mit (weiterer) Cyber-Spionage bedroht würde. Das Eindringen in Computersysteme zur Informationsbeschaffung ist längst ein Mittel der Außenpolitik. Hier stellt sich die Frage, ob das Ziel von Computerspionage neben technischen und nachrichtendienstlichen Mitteln auch über rechtliche Möglichkeiten zur Abwehr verfügt, die Spionagetätigkeit anderer Regierungen also gegen internationales Recht verstößt. Insbesondere ist fraglich, ob die Durchführung von Computerspionage ein Kriegsgrund für das Opfer sein kann.

Eine explizite Erlaubnis für Spionage kennt das Internationale Recht nicht. Sie lässt sich auch nicht dem Gewohnheitsrecht entnehmen: Zwar dürften alle Staaten Spionageprogramme unterhalten und damit eine solide Staatenpraxis schaffen; eine entsprechende Rechtsüberzeugung lässt sich daraus jedoch nicht ableiten. Im Gegenteil wird Spionage verurteilt bzw. geleugnet, sodass einer Überzeugung hin zur Legalität von Spionage widersprochen wird. Ebensowenig aber gibt es ein Verbot – von einer Ausnahme (Unantastbarkeit von Archiven und Korrenspondenz von Botschaften und diplomatischen Missionen) im *self-contained regime* des Diplomatenrechts abgesehen. Auch die Tatsache, dass wohl alle Staaten Spionage *gegen sich selbst* in ihrem nationalen Recht unter Strafe stellen, lässt sich nicht für einen allg. Rechtsgrundsatz i.S.d. Art. 38 (1) c) IGH-Statut gegen Spionage verwenden: Die Staaten schützen jeweils sich selbst, nicht aber andere Staaten vor Spionage. Im Ergebnis wird man, nach dem *Lotus-Prinzip*, Spionage als „nicht verboten" ansehen müssen. Dennoch stellt sie eine Verletzung der Interessen des Zielstaates dar, auch wenn diese Interessen zunächst rechtlich nicht geschützt werden. Für rechtliche Gegenmaßnahmen müsste diese Verletzung der Interessen das Ausmaß einer Rechtsverletzung annehmen; für bewaffnete Gegenwehr sogar einer Situation gleichkommen, die ein Staat mit militärischen Mitteln beantworten darf.

Grundsätzlich als Anwendung oder Androhung von Gewalt, insb. als bewaffneten Angriff wird man „Cyber-Spionage" nicht qualifizieren können. Bewaffnete Gegenmaßnahmen scheiden daher aus. Auch, wenn die Cyber-Sicherheitsstrategien mehrerer Staaten und auch der NATO die Nutzung militärischer Mittel zur Beantwortung von „Cyber-Angriffen" durchaus mit einbeziehen, können damit nur Angriffe gemeint sein, die die Ergebnisse von Spionage höchstens ausnutzen; nicht aber bereits die Spionage selbst. Dass bloße Spionage bereits die Ausmaße und Folgen (*scale and effects*) eines Angriffs mit konventionellen Waffen erreichen könnte, ist unrealistisch.

Schon eher könnte man eine Verletzung der territorialen Integrität des Zielstaates annehmen. Zwar dürften sich solche Spionagetätigkeiten selten physisch manifestieren (was ein klarer Rechtsbruch wäre), dennoch entfalten sie auch beim bloßen heimlichen Kopieren von Daten eine Wirkung auf den Systemen des Zielstaates. Es überzeugt nicht, dass der Standort eines Agenten am Kopierer im Zielstaat oder am Computer im Heimatstaat relevant sein soll, wenn es um den „Diebstahl" von Staatsgeheimnissen geht. Diese Ansicht hat sich indes auf internationaler Ebene bislang nicht durchsetzen können. Zu beobachten wäre in nationaler Perspektive, ob die Bundesregierung die Vorkommnisse zum Anlass nimmt, eine Entwicklung des Völkerrechts hinsichtlich einer Eindämmung von Computer-Spionage anzustoßen. Angesichts des offenen Gleichmuts aber, mit dem sie das systematische Abhören wohl nahezu der gesamten Bevölkerung der Bundesrepublik hinnimmt, darf das allerdings bezweifelt werden.

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. Die BOFAXE werden vom Deutschen Roten Kreuz unterstützt.