Nr. 496D
10.07.2017

BOFAXE

Liebesgrüße an die Ukraine

Autor / Nachfragen

Stephan Kolossa
Wiss. Mit. am Institut für Friedenssicherungsrecht und Humanitäres Völkerrecht (IFHV) und Mitglied des SecHuman-Fortschrittskollegs

Nachfragen:
stephan.kolossa@rub.de

Webseite

http://www.ifhv.de

http://www.sechuman.rub.de

Fokus

Vor zwei Wochen hat eine Cyber-Operation Computersysteme auf der ganzen Welt verschlüsselt und damit für mehrere Tage unbrauchbar gemacht. Dabei traf es die Ukraine am stärksten. Begründete Vermutungen sehen die Urheberschaft bei Russland. Jedoch selbst wenn man Russland als maßgeblichen Akteur ansieht, liegt kein Verstoß gegen das Gewaltverbot vor.

Quellen:

https://www.theguardian.com/technology/2017/jun/27/petya-ransomware-cyber-attack-who-what-why-how.

https://www.nytimes.com/2017/06/28/business/ramsonware-hackers-cybersecurity-petya-impact.html?mcubz=2.

Vor zwei Wochen legte ein Cyber-Angriff Computersysteme auf der ganzen Welt lahm. Als erstes und am stärksten betroffen war die Ukraine. In der Hauptstadt Kiew sorgte der Angriff dafür, dass die EDV-Systeme von Ministerien, Stromversorgern, Banken, Metrostationen und dutzenden weiteren Stellen verschlüsselt und damit für mehrere Tage funktionsuntauglich wurden. Danach breitete sich das Schadprogramm auf einzelne Unternehmen u.a. in Europa, Australien und den USA aus. In technischer Hinsicht ähnelt das Programm dem Verschlüsselungstrojaner „WannaCry“ und ist grundsätzlich als sog. Ransomware einzustufen, d.h. das betroffene Dateien erst nach Zahlung eines Lösegeldes, das typischerweise in der rein elektronischen Bitcoin-Währung zu zahlen ist, von den Angreifern wieder freigegeben werden. Durch mathematische Kalkulationen oder ein systematisches Ausprobieren von Entschlüsselungscodes (sog. Brute-Force-Methode) kann der Verschlüsselungsmechanismus regelmäßig nicht überwunden werden. Eine Besonderheit im vorliegenden Fall liegt darin, dass es den Angreifern aufgrund der Art der konkreten Lösegeldforderungen nicht auf das Lösegeld angekommen sein kann, sondern allein auf die Verschlüsselung und die Unbrauchbarmachung der Daten.

Geht man mit der vor allem in der Ukraine vorherrschenden Ansicht davon aus, dass der Angriff von der Russischen Föderation gelenkt wurde und gezielt gegen den ukrainischen Staat gerichtet war, hätte Russland nach geltendem Völkerrecht wohl trotz des Ausmaßes des Angriffs nicht gegen das Gewaltverbot (vgl. Art. 2 Nr. 4 VN-Charta) verstoßen. Ob eine Cyber-Operation als Anwendung von Gewalt zu werten ist, entscheidet sich durch einen Vergleich mit konventionellen militärischen Mitteln oder deren Auswirkungen. Die überzeugende (wohl) herrschende Meinung stellt bei einem solchen Vergleich vor allem auf die konkreten Auswirkungen der Cyber-Operation ab, wobei auch bereits die Art des Ziels von Bedeutung ist. Dieses Vorgehen findet sich ebenfalls in Regel 69 des *Tallinn Manual 2.0*, das ein internationales Expertengremium des *Cooperative Cyber Defence Centre of Excellence* der NATO verfasst hat, jedoch eo ipso rechtlich unverbindlich ist. Danach gilt, dass bloße computerinterne Auswirkungen regelmäßig nicht als Anwendung von Gewalt einzustufen sind, solche, die real-physische Schäden an Personen oder Sachen hervorrufen, regelmäßig schon.

Im vorliegenden Fall ist aufgrund der Gesamtschau der Auswirkungen nicht von einer Gewaltanwendung auszugehen. Zunächst wurde weder die physische Integrität der betroffenen Computersysteme, also die Hardware angegriffen noch ist es zu Personenschäden gekommen. Auch ein Angriff auf kritische Infrastrukturen allein reicht für die Annahme von Gewaltanwendung nicht aus. Das Programm hat die alltägliche Regierungsarbeit erschwert und behindert, jedoch wird diese Auswirkung als Unannehmlichkeit einzustufen sein. Auch eine vorübergehende Funktionslosigkeit von Bankautomaten hat die Gesellschaft der Ukraine nicht etwa in ein vernichtendes Chaos gestürzt. Ferner trägt das Argument nicht, dass die Stelle, die an dem ehemaligen Atomreaktor in Tschernobyl die radioaktive Strahlung misst, ihre automatischen Messungen nicht mehr durchführen konnte. Denn es handelt sich gerade nicht um ein aktives Atomkraftwerk wie bei dem Stuxnet-Angriff auf tatsächlich aktive iranische Atomanlagen, sondern um eine reine Überprüfungsstelle, die die aktuelle radioaktive Strahlung misst und die nun von Hand betrieben werden musste. Letztlich wurde der Angriff auch nicht mittels eines Programms ausgeführt, das besondere Hochsicherheitsstrukturen gebrochen hat, sondern durch Ausnutzung einer monatelang bekannten Sicherheitslücke im Windows-Betriebssystem.

Da es sich bei der Cyber-Operation insgesamt nicht um einen Verstoß gegen das Gewaltverbot handelt, scheidet auch die Einordung der Operation als bewaffneter Angriff im Sinne des Art. 51 VN-Charta aus. Diese Einordnung bedeutet jedoch nicht, dass die Cyber-Operation als völkerrechtskonform angesehen werden kann. Bei der Frage nach der weiteren Vereinbarkeit mit geltendem Völkerrecht wäre besonders die Autorenschaft Russlands genau zu untersuchen, da diese keineswegs auf der Hand liegt. Des Weiteren hoch umstritten ist die Frage nach der Legalität von Gegenmaßnahmen gegen Angriffe unterhalb der Schwelle von Gewaltanwendungen wie im vorliegenden Fall, was sich nicht zuletzt an dem Ergebnis der speziell eingesetzten *UN Group of Governmental Experts* gezeigt hat, das sich trefflich als Einigkeit zur Uneinigkeit bezeichnen lässt.

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.