Sachstand

Autorisierung von Militäroperationen durch den VN-Sicherheitsrat nach Art. 42 VN-Charta und Cyber-Operationen

Autorisierung von Militäroperationen durch den VN-Sicherheitsrat nach Art. 42 VN-Charta und Cyber-Operationen

Aktenzeichen: WD 2 - 3000 - 091/17
Abschluss der Arbeit: 5. Oktober 2017
Fachbereich: WD 2: Auswärtiges, Völkerrecht, wirtschaftliche Zusammenarbeit und Entwicklung, Verteidigung, Menschenrechte und humanitäre Hilfe

Inhaltsverzeichnis

1. Mandatierung von Militäroperationen durch den VN-Sicherheitsrat

Art. 42 der VN-Charta legt fest, dass der VN-Sicherheitsrat unter bestimmten Voraussetzungen „mit Luft-, See- oder Landstreitkräften die zur Wahrung oder Wiederherstellung des Weltfriedens und der internationalen Sicherheit erforderlichen Maßnahmen *durchführen kann*". Eine Durchführung solcher Maßnahmen durch den VN-Sicherheitsrat *selbst,* wie der Wortlaut von Art. 42 der VN-Charta nahelegt, findet mangels eigener Truppen des Sicherheitsrates in der VN-Praxis nicht statt; vielmehr **autorisiert** der Sicherheitsrat die VN-Mitgliedstaaten lediglich, **solche Maßnahmen durchzuführen**.

Dabei verwendet er in seinen Resolutionen (Art. 25 VN-Charta) regelmäßig die Formulierung „*to use all necessary means*",[1] was den Einsatz sowohl von Luft-, See- als auch von Landstreitkräften beinhaltet. Eine **Beschränkung der Autorisierung auf bestimmte Teilstreitkräfte nimmt der VN-Sicherheitsrat in der Praxis nicht vor**. Die Staaten **entscheiden vielmehr in eigener Verantwortung** und entsprechend ihren politischen und verfassungsrechtlichen Vorgaben sowie militärischen Fähigkeiten, in welcher Form sie an VN-mandatierten Militäroperationen teilnehmen wollen (z.B. nur Lufteinsätze oder auch Bodentruppen).

2. Computernetzwerkoperationen und Völkerrecht

Computernetzwerkoperationen (CNO) beschreiben Handlungen im Bereich des Cyber-Informationsraums, die sowohl defensiver als auch offensiver Natur sein können. Auch wenn der **Cyber-Raum** in der politischen Diskussion oft als „**fünfter strategischer Raum**" (neben Luft, Land, See und Weltraum) bezeichnet wird, lassen sich **digitale Wirkmittel** im **Cyber- und Informationsraum**, je nachdem, von *wem* sie eingesetzt werden, einer der traditionellen Teilstreitkräfte zuordnen. Die IT-Spezialisten des **Kommando Cyber- und Informationsraum** (KdoCIR) der Bundeswehr bilden keine eigene Teilstreitkraft der Bundeswehr.

Das von einer internationalen Expertengruppe im **NATO Cooperative Cyber Defence Centre of Excellence** in Tallinn ausgearbeitete sog. "**Tallinn Manual**"[2] bildet den derzeit herrschenden Meinungsstand zu Fragen des *cyberwar* in Wissenschaft und Praxis ab. Das *Tallinn Manual* plädiert dafür, **Computernetzwerkoperationen den allgemeinen Regeln des Völkerrechts** (insbesondere des humanitären Völkerrechts, aber auch dem *ius ad bellum*, also insb. Kapitel VII der VN-Charta) **zu unterwerfen,** und wendet sich – mangels Notwendigkeit – **entschieden dagegen, für den Cyber-Raum ein eigenständiges Rechtsregime zu schaffen**. Dies entspricht auch der politischen Auffassung im Bundesverteidigungsministerium.

---

1 Stellvertretend für alle nachfolgenden Resolutionen vgl. SR-Res. 678 (1991) zur Befreiung Kuwaits von der Irakischen Annexion.

2 *Schmitt, Michael* (Hrsg.), Tallinn Manual on the international law applicable to cyber warfare, Cambridge Univ.-press 2013, https://www.jku.at/intlaw/content/e275831/e275836/e276629/Tallinn_Manual_CW.pdf. Mittlerweile erschienen ist das Tallinn Manual 2.0, Cambridge, 2. Aufl. 2017.

3. Auslegung der VN-Charta

Als die VN-Charta im Jahre 1945 verabschiedet wurde, waren sog. Computernetzwerkoperationen noch unvorstellbar. Gleichwohl lässt sich die VN-Charta als „living instrument“ **dynamisch-evolutiv interpretieren**, was nahelegt, **bestimmte technische Entwicklungen** vor allem im Waffenbereich in diese Interpretation mit einzuschließen. Dies gilt nicht nur für Cyber-Fähigkeiten, sondern z.B. auch für militärische Weltraumfähigkeiten einschließlich Raketentechnik oder für nukleare oder biologische Fähigkeiten.

Das *Tallinn Manual* führt insoweit aus:

> „While Art. 42 indicates that enforcement measures may be taken by air, sea or land forces of members of the UN, the International Group of Experts agreed that any action undertaken on the basis of this Rule may be implemented by, or against, cyberspace capabilities” (Rule 18, No. 9).
>
> “The phrase ´all necessary means` implies the authority [of the UN-Security Council] to employ cyber operations against the State or entity that is the object of the resolution in question” (Rule 18, No. 7).

In der Praxis des Sicherheitsrats hat es bislang keinen Fall einer solchen Autorisierung von Cyberoperationen gegeben. Es sind auch kaum Fälle vorstellbar, in denen Cyber-Wirkmittel sinnvollerweise *isoliert* gegen potentielle Aggressoren eingesetzt werden. Das **Kommando Cyber- und Informationsraum** (KdoCIR) der Bundeswehr betrachtet Cyberfähigkeiten (nur) als „unterstützendes, komplementäres Wirkmittel“. CNO werden damit regelmäßig **impliziter Teil eines vom VN-Sicherheitsrat bzw. vom Bundestag mandatierten Militäreinsatzes sein**.

4. Praxis und offene Fragen

In der VN-Praxis hat es bislang **noch keinen Fall** gegeben, in dem der Sicherheitsrat eine CNO als **Bedrohung des Friedens i.S.v. Art. 39 VN-Charta** qualifiziert hat. Dies führt zu der nach wie vor rechtlich nicht abschließend gelösten Frage, **wann eine Cyber-Attacke die Schwelle zum bewaffneten Angriff** („*armed attack*“) i.S.v. Art. 51 VN-Charta **überschreitet**.

In der völkerrechtlichen Literatur wird darüber diskutiert, ob das staatliche **Selbstverteidigungsrecht** auch gegen **Cyber-Attacken von nicht-staatlichen Akteuren** (private Hacker) ausgeübt werden darf. Damit zusammen hängt die sowohl technisch als auch rechtlich problematische Frage nach der sog. **Attribution** (kommt der Angriff aus dem In- oder aus dem Ausland?). Weiter ist rechtlich umstritten, wie ein Staat **auf Cyberattacken reagieren** darf (nur digital oder auch „kinetisch“).

5. Weiterführende Literatur

Zum **Thema *Cyberwar*** existieren mittlerweile schon zahlreiche Publikationen worden. Einen völkerrechtlichen Einstieg bieten u.a. die Werke von:

- *Sven-Hendrik Schulze*, Cyber-"War" - Testfall der Staatenverantwortlichkeit, Tübingen, 2015.
- *Eric Boylan,* Applying the law of proportionality to cyber conflict: Suggestions for practitioners, in: Vanderbilt journal of Transnational Law 2017, S. 217-244.
- *Thomas Reinhold*, Cyberspace als Kriegsschauplatz? : Herausforderungen für Völkerrecht und Sicherheitspolitik, in: Aus Politik und Zeitgeschichte: Beilage zur Wochenzeitung Das Parlament, Nr. 66 (2016) vom 29.8.2016, S. 22-27.
- *Katharina Ziolkowski* (ed.), Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy, NATO Publication, Tallinn 2013.
- Gutachten WD 2 – 3000 – 038/15 vom 24.2.2015, „Anwendbarkeit des humanitären Völkerrechts auf Computernetzwerkoperationen und digitale Kriegsführung.“ (**Anlage**)

Aus **verfassungsrechtlicher Sicht** zur Frage von Cyberoperationen als **Inlands- bzw. Auslandseinsätze der Bundeswehr**:

- *Christian Marxsen,* Verfassungsrechtliche Regeln für Cyberoperationen der Bundeswehr. Aktuelle Herausforderungen für Einsatzbegriff und Parlamentsvorbehalt, in: JZ 2017, S. 543 ff.[3]

Hinzuweisen ist schließlich auf die **Öffentliche Anhörung im Verteidigungsausschuss des Deutschen Bundestages** am 22. Februar 2016 zum Thema

> „Die Rolle der Bundeswehr im Cyberraum - Verfassungs-, völker- und sonstige nationale und internationale rechtliche Fragen sowie ethische Aspekte im Zusammenhang mit Cyberwarfare und die hieraus erwachsenden Herausforderungen und Aufgaben für die Bundeswehr“.[4]

* * *

[3] Verfügbar online unter: http://www.ingentaconnect.com/contentone/mohr/jz/2017/00000072/00000011/art00002?crawler=true&mimetype=application/pdf.

[4] https://www.bundestag.de/presse/pressemitteilungen/2016/neuer-inhalt/407780.