Jean-Christophe Noël: What Is Digital Power? Paris: Ifri, November 2019

Besprochen von **Martin Eduard Debusmann**, LL.M. MPhil MA, Strategic Advisor bei PwC Strategy&, Alumnus der Bundesakademie für Sicherheitspolitik. Zürich, Schweiz, E-Mail: martin.debusmann@strategyand.ch.pwc.com

<https://doi.org/10.1515/sirius-2020-2028>

Der ehemalige Offizier der *Armée de l'Air Française*, Jean-Christophe Noël, gibt mit seiner Studie einen Ansatz zur Definition „digitale Macht“ (digital power). Digitale Macht sei die Fähigkeit eines Akteurs, das Verhalten anderer Akteure in internationaler Dimension durch die Anwendung digitaler Daten zu beeinflussen. Dazu müsse er ein günstiges Ökosystem schaffen, Daten und Netzwerke kontrollieren und die eigenen digitalen Fähigkeiten mit solchen aus der analogen Welt koordinieren können. Digitale Macht kombiniere zahlreiche denkbare (und sich teils widersprechende) Facetten: Sie sei beispielsweise sowohl konventionell als auch netzwerk-orientiert, befreiend und überwachend, asymmetrisch und begrenzt.

Der Autor zeigt die Schwierigkeit auf, digitale Macht mit den bestehenden Definitionen und Kategorien von Macht zu erklären. So gäbe es bei digitaler Macht beispielsweise keinen definierbaren Raum im Sinne eines (geographischen) Gebietsanspruches. Ob es sich bei Cyberspace um einen macht-definitorisch abgrenzbaren Raum handele, sei umstritten. Noël schlägt daher vor, digitale Macht in Bezug auf Netzwerke statt auf Räume zu verstehen. Macht-

volle Netzwerke habe es in der Geschichte schon immer gegeben. Der Autor erwähnt unter anderem die Seebünde des antiken Griechenlands oder die maritimen Verbindungen zur Entdeckung der Neuen Welt. Der Cyberspace als Netzwerk werde nicht nur von Staaten, sondern auch von Firmen und Individuen geformt, wodurch Staaten kein Machtmonopol errichten könnten.

Noël wendet sich in einem nächsten Schritt den Abläufen (*practices*) des Cyberspaces zu: Wesentliches Element einer Definition digitaler Macht müsse die Art der Nutzung digitaler Ressourcen im Cyberspace sein. Von daher sei Angriffssoftware bedeutend. Diese sei nur einmal einsetzbar (*one-strike weapon*): Mit einem (Erst-) Einsatz werde sie für den Gegner entdeckbar, so dass dieser sie analysieren und Gegenmaßnahmen entwickeln könne. Gleichfalls müsse der Angreifer entscheiden, ob er sich zu erkennen geben wolle oder ob er riskiere, dass der Gegner den Angriff gar nicht als solchen (oder als einen eines anderen, vermeintlichen Gegners) identifiziere und damit die gewünschte Machtdemonstration verpuffe. Machtdemonstration und Machteffizienz stünden daher im Cyberspace in einem erheblichen Zielkonflikt.

Digitale Macht, zwischenzeitlich von Noël nicht nur als *digital power* sondern auch als *Cyberpower* bezeichnet, habe die Interessens- und Motivationslage von Staaten und Individuen nicht verändert, sondern trage zu der Vielfalt der Ausprägungen von Wettbewerb und Konfrontation bei. Daher bestünde die Herausforderung darin, digitale Macht mit den Mitteln konventioneller militärischer Macht zu verbinden, wobei letztere eine Einschränkung ersterer darstellen könne: Digitale Supermächte wie China und Russland würden beispielsweise einen offenen digitalen Konflikt mit den USA meiden, weil sie deren Reaktion mittels konventioneller Militäreinsätze befürchteten.

Noël führt aus, wieso Offensivmaßnahmen das bevorzugte Mittel im Einsatz von digitaler Macht darstellten: Der Zugang zum Netzwerk des *Cyberspace* sei erschwänglich und einfach herzustellen, das Kosten-Wirkungs-Verhältnis sei vergleichsweise niedrig. Fehlschläge, selbst wenn diese einem Aggressor zurechenbar seien (*naming and shaming*), hätten geringe Konsequenzen eines Gegenangriffs. Das angegriffene System sei einfach im Netzwerkverbund identifizierbar, während der Angreifer verdeckt operieren könne. Letztlich könne sich der Verteidiger nicht auf alle erdenklichen Angriffsszenarien vorbereiten.

Nicht nur nicht-staatliche Akteure seien Teil des *Cyberspace*, auch Konfliktmethoden aus der Wirtschaftswelt spielten vermehrt eine Rolle. So ginge es bei digitaler Macht vorrangig nicht darum, einen vernichtenden (Erst-) Angriff auf den Gegner zu starten, sondern dessen Infrastruktur zu infiltrieren, für die eigenen Interessen zu

nutzen und auf Wunsch zu lähmen. Das Spielfeld digitaler Macht sei daher die Grauzone zwischen Krieg und Frieden.

Vor allem im Bereich der politischen Kriegsführung (*political warfare*, von George Kennan in Anlehnung an Clausewitz' „Der Krieg ist eine bloße Fortsetzung der Politik mit anderen Mitteln“ entwickelt) spiele digitale Macht eine Rolle, indem direkt auf die Beeinflussung der Wahrnehmung und die politische Einstellung der Zivilbevölkerung gezielt werde. Sie werde in dieser Form unter anderem von Unternehmen (wie *facebook*) durch die Sammlung und Nutzung von Daten ausgeübt. Digitale Macht könne dabei ihr Ziel kontrollieren und diesem das Gefühl vermitteln es sei zufrieden. Sie setze auf eine Kontrolle des Geistes statt des Körpers und könne daher ein Abwenden von Gewalt darstellen.

Noël verweist auf die bisherige Entwicklungsgeschichte der Digitalisierung. Digitale Macht, so der Verfasser, entwickle sich kontinuierlich mit neuen Erfindungen fort und hänge unabdingbar mit dem Verfügen über *state-of-the-art*-Technologien zusammen. Er zeigt ebenfalls Herausforderungen von Ansätzen einer Regulierung auf. In seiner Zusammenfassung erwähnt Noël staatliche, erst recht sicherheitspolitische und militärische, Komponenten digitaler Macht nicht mehr, sondern widmet sich bevorzugt den Problemen des Individuums hinsichtlich der Kontrolle seiner digitalen Daten.

<https://www.ifri.org/en/publications/etudes-de-lifri/what-digital-power>