Metis

Studie

Abschreckung im 21. Jahrhundert

Nr. 16 | Mai 2020

Institut für
Strategie & Vorausschau

Zusammenfassung

Auf den ersten Blick fußt Abschreckung auf einer einfachen Idee: Ein Akteur droht möglichen Angreifern glaubhaft Vergeltung an. Er überzeugt sie auf diese Weise, dass die Kosten einer Aggression den Nutzen übersteigen. So verhindert Abschreckung Kriege. Auf den zweiten Blick wirft das Konzept schon seit Beginn des Atomzeitalters Fragen auf. Die vorliegende Studie prüft im Lichte aktueller sicherheitspolitischer Herausforderungen, ob und wie es noch anwendbar ist.

Das Konzept der Abschreckung

Abschreckung ist als Konzept durchgehend in der Geschichte politischer und militärischer Auseinandersetzungen anzutreffen. Aber erst im Kalten Krieg gewann es – in Gestalt der nuklearen Abschreckung – akademisch und praktisch seine bis heute anhaltende, hervorgehobene Bedeutung. Abschreckung kann auf zwei Arten, durch Androhung einer Bestrafung (*deterrence by punishment*) oder durch Verweigerung der Erfolgsaussichten (*deterrence by denial*), erfolgen. Ziel eines Staates A im ersten Fall ist es, Staat B glaubhaft zu signalisieren, dass eine bestimmte Handlung oder ein Angriff rasche Vergeltung durch Staat A samt der Zerstörung essenzieller Werte in Staat B zur Folge haben wird. Im zweiten Fall demonstriert Staat A gegenüber Staat B Widerstand und verdeutlicht so, ohne eine Androhung von Vergeltung, dass die politischen und militärischen Ziele mittels eines Angriffs nicht erreichbar sind. Die beiden Modelle sind nicht trennscharf.

Abschreckung wird häufig im Sinne einer strategischen Ambiguität praktiziert. So war während des Kalten Krieges strategische Ambiguität aus Sicht der USA etwa mit Blick auf Deutschland attraktiv. Die Verteidigung des isolierten West-Berlins war nicht praktikabel. Dessen Schutz wurde daher durch die Androhung von Vergeltungsmaßnahmen anderswo gewährleistet. Wo und wie groß solche Reaktionen ausfallen würden, das war der Sowjetunion unbekannt. Zurückhaltung in Moskau war die Folge.

Das Beispiel verdeutlicht zugleich die „erweiterte Abschreckung", die das Verhindern von Angriffen auf Dritte zum Ziel hat – zum Beispiel Verbündete oder Partnerstaaten, wie im Falle des US-Nuklearschirms über Europa oder auch den US-Sicherheitsgarantien in Asien. „Direkte Abschreckung" dient hingegen nur dazu, Angriffe auf das eigene Territorium zu verhindern. Besteht wechselseitige Abschreckung zwischen zwei Akteuren, die beide überzeugt sind, dass sie ihr Gegenüber in einem Vergeltungsschlag sicher zerstören können (*mutual assured destruction*), ist vom Zustand der strategischen Stabilität die Rede.

Abschreckung stellt sich nicht von alleine ein. Die „delikate Balance" muss mit politischen und militärischen Mitteln hergestellt werden. Ihr Effekt ist systemisch, wirkt sich also auf zwischenstaatliche Verhältnisse aus. Aber ausschlaggebend für ihr Funktionieren ist die Beeinflussung von (individuellen) Entscheidungsträgern.

Theorie und Praxis der Abschreckung

Die akademische und theoretische Beschäftigung mit dem Konzept der Abschreckung kam mit der sogenannten ersten Forschungswelle nach dem Zweiten Weltkrieg aufgrund der Notwendigkeit auf, dem Atomzeitalter politisch zu begegnen. Bereits damals wurden die eingangs skizzierten Kernkonzepte entwickelt – ganz offenkundig stark beeinflusst von der bipolaren Ordnung des Kalten Krieges. Die erste Welle hob auf den „Schrecken" der Abschreckung ab, sprach also buchstäblich davon, dem Gegenüber Angst einzujagen.

Die zweite Forschungswelle in den 1950er und 1960er Jahren entemotionalisierte das Konzept. Die Angst wurde aus dem Vokabular gestrichen, und stattdessen wurden rationale Akteure, Kosten-Nutzen-Kalküle und Modellierungen mittels Spieltheorie eingeführt in der Absicht,

allgemeingültige Aussagen über Nuklearstrategien abzuleiten. Der bis heute bestehende Mainstream der Abschreckungstheorie, explizit verstanden als „Manipulation des gegnerischen Kosten-Nutzen-Kalküls", geht auf diese einflussreichen Arbeiten zurück. Auch das Schlüsselkonzept der „Eskalationsdominanz", also selbst stets den einen, entscheidenden, letztendlich abschreckenden Schritt weiter gehen zu können, geht auf diese Phase zurück.

In der dritten Welle ab den 1970er Jahren wurde kognitive Psychologie herangezogen und anhand von Fallstudien überprüft, ob reale Entscheidungsträger tatsächlich wie rationale Akteure handeln: Es zeigte sich, dass die Annahmen der zweiten Welle nur begrenzt Gültigkeit beanspruchen konnten, weil in der Realität Fehlwahrnehmungen, Waghalsigkeit, Ideologie bis hin zu Drogeneinfluss von Entscheidungsträgern dem, was man als rationales Kalkül verstand, zuwiderliefen. Empirische Studien offenbarten darüber hinaus, dass Entscheidungsträger auch aus innerstaatlichen Beweggründen, etwa zur eigenen Machterhaltung, der Abschreckungsdrohung trotzend den Konflikt suchten. In Summe legte die empirische Analyse von Abschreckungsstrategien nahe, dass das Konzept das Risiko birgt, genau den Krieg herbeizuführen, den es eigentlich verhindern soll. Mit anderen Worten: Man hatte das in der Abschreckungstheorie inhärente Paradox – dass ihretwillen permanent vorbereitet und glaubhaft angedroht werden muss, was doch eigentlich niemals stattfinden soll – in der Praxis wiedergefunden.

Abb. 1 *Permanente Konfrontation: Abschreckung sieht die glaubwürdige Androhung von Vergeltung vor, um kriegerische Eskalation zu verhindern (Checkpoint Charlie, 1961).*

Eine vierte Welle reagierte nach dem Ende des Kalten Krieges auf den Rückgang zwischenstaatlicher Kriege, den Anstieg innerstaatlicher Konflikte und das Phänomen des internationalen Terrorismus. Asymmetrische Akteurskonstellationen und sogenannte „Schurkenstaaten" rückten in den Blick – erneut wurden, in der Diskussion um Motive von Selbstmordattentätern und Wertvorstellungen von Autokraten, die westlichen Vorstellungen von Rationalität in der *Mainstream*-Abschreckungstheorie hinterfragt. Aktuell ist von einer fünften Welle die Rede, die für ein Sammelsurium von Ansätzen steht, das quasi tagesaktuell nicht-kinetische, cyberspezifische, terroristische und hybride Risiken mit diplomatischen, wirtschaftlichen, politischen und militärischen Mitteln adressieren soll, damit aber nur mehr analytische Konfusion rund um das Konzept der Abschreckung erzeugt. Längst droht, auch angesichts der seit dem Kalten Krieg nicht thematisierten Paradoxien und problematischen Grundannahmen, eine konzeptionelle Überdehnung, die im Begriff ist die Idee der Abschreckung ad absurdum zu führen.

(Quelle: wikimedia)

Abschreckung in neuen Räumen?

Die „klassische" Abschreckungstheorie des Kalten Krieges und ihre Anwendung in der Praxis war, wenngleich nicht so verlässlich und verallgemeinerbar wie während der zweiten Welle erhofft, zweifellos nicht ohne Effekt. Dass sie das Verhalten zwischen Nuklearwaffenstaaten reguliert, lässt sich schwerlich bestreiten, auch wenn vielleicht bis heute nicht verstanden sein mag, wann wie viel rationales Kalkül oder doch blanke Angst im Spiel ist. Im Falle neuer sicherheitspolitischer Herausforderungen sticht allerdings ins Auge, dass bereits einige der grundlegenden Voraussetzungen für das Funktionieren von Abschreckung nicht gegeben sind.

Im Informationsraum werfen Cyberangriffe die Frage auf, ob diese sich abschrecken lassen. Das Hauptproblem bei der Anwendung von Abschreckung im Cyberraum ist das sogenannte Attributionsproblem, also die fehlende Möglichkeit, den Urheber eines Cyberangriffs eindeutig zu bestimmen. Wenn ein Staat einen Angreifer lokalisieren kann, beispielsweise in einem Internetcafé oder Privathaushalt in Asien, wäre diese Information nur bedingt hilfreich um auf den Angriff tatsächlich ausführenden Akteur zu schließen. Selbst wenn der Angriff auf ein Rechenzentrum eines lokalen Militärs zurückgeführt würde, bliebt das Risiko bestehen, dass Elemente der Cyberarchitektur des vermeintlichen Verursacherstaats in Wahrheit durch Dritte kompromittiert wurden. Diese Problematik wird zunehmend komplexer, da einige Staaten nicht-staatliche Akteure für Operationen im Cyberraum beauftragen. Dadurch kann der angegriffene Staat auch mit ausgereifter Cyberintelligence die glaubhafte Abstreitbarkeit (*plausible deniability*) des vermeintlichen Verursacherstaats nur schwer oder nur nach sehr zeitintensiven forensischen Untersuchungen entkräften. Die Androhung einer raschen Vergeltung im Sinne der *deterrence by punishment* läuft somit mangels Adressaten ins Leere.

Durch die Anstrengungen staatlicher Akteure, den Cyberraum und kritische Infrastrukturen gegen Cyberangriffe zu schützen, hat sich in den letzten Jahren die Hürde für erfolgreiche Cyberangriffe stark erhöht. Gegnerische Netzwerkoperationen müssen mehr Ressourcen, Energie, Personal und Zeit aufwenden, um einen erfolgreichen Angriff auf staatliche Schlüsselkapazitäten durchzuführen. Ein Angriff auf militärische Strukturen mit einem Laptop aus dem Internetcafé ist höchstens in Hollywoodfilmen plausibel. Somit kann davon ausgegangen werden, dass zumindest *deterrence by denial* gegen eine Vielzahl ressourcenschwacher Akteure erfolgreich angewendet werden kann. Das Konzept der Resilienz spielt hier eine hervorgehobene Rolle, wie im Folgenden noch weiter ausgeführt werden wird.

Für den Weltraum werden zum einen Szenarien aufgeworfen, die die Anwendbarkeit klassischer Abschreckungskonzepte in Zweifel ziehen. Zum anderen ergeben sich mit der militärischen Nutzung des Weltraums neue Szenarien, in denen die „delikate Balance" am Boden tangiert würde.

Zu Zeiten des Kalten Krieges war die Gruppe der „üblichen Verdächtigen" im Orbit mangels Verbreitung von Weltraumkapazitäten sehr überschaubar. Durch das Vordringen privater Akteure besteht hier nun mit Blick auf kinetische Wirkungen ein Attributionsproblem, welches – wie oben geschildert – im Falle nicht-kinetischer Operationen schon länger Bestand hatte. Auch hier läuft die gängige Abschreckungspraxis ins Leere.

Neue Weltraumfähigkeiten wie Anti-Satellitenraketen oder andere Wirkmittel[1] können zudem etwa die Früherkennung eines nuklearen Erstschlags oder sogar die nukleare Zweitschlagfähigkeit gefährden, also die strategische Stabilität unterminieren. Die Abschreckungslogik wäre in diesem Fall intakt. Es ergeben sich allerdings neue Risiken für ihre Wirkung als stabilem Garant für den anhalten Nichtgebrauch von Nuklearwaffen. So wäre zum Beispiel denkbar, dass ein Nuklearwaffenstaat einen Angriff auf seine weltraumgestützten Fähigkeiten mit nuklearer Vergeltung – im Sinne eines *use them or lose them* – zu beantworten, um einer Außerkraftsetzung seiner Zweitschlagfähigkeit zuvorzukommen.

Abschreckung als Resilienz?

Die Abschreckung begleitet die Menschheit in Theorie und Praxis also ins 21. Jahrhundert, wenngleich dabei alte und neue Fragen aufgeworfen werden. Eine vielversprechende, vorausschauende Überlegung besteht darin, über Abschreckung insbesondere in neuen Anwendungsbereichen radikal vereinfacht und im Sinne von Resilienz nachzudenken – wodurch man sich nebenbei auch dem Abschreckungsparadox und anderer Altlasten der Abschreckungstheorie, wie etwa dem stets schwelenden Problem der Glaubwürdigkeit, entledigt. Ein solcher Denkanstoß würde die Grundlogik der *deterrence by denial* zum Ausgangspunkt nehmen.

Die Idee dabei bliebe, einem potenziellen Angreifer die Sinnlosigkeit seines Unterfangens zu verdeutlichen, weil es offenkundig keinen Erfolg verspricht. Aber während dazu in der klassischen Abschreckungstheorie im Sinne eines *deterrence by denial*, mit dem Risiko der Fehlwahrnehmung, Signale im militärischen Kontext gesendet werden müssen, würde eine *deterrence by resilience* einfach aus Robustheit und der demonstrierten Fähigkeit zur Absorption von Angriffen erwachsen. Es geht also nicht um Abwehr und Gegenangriff in Reaktion auf, beispielsweise, hybride Angriffe, sondern, in Anlehnung an gängiges Abschreckungsvokabular, um das Entwickeln von „Absorptionsdominanz" und damit das Beherrschen der Schadensentfaltung sowie der zeitlichen Dimension zwischen Angriff und Rückkehr zum *status quo ex ante*. Wenn Staat A also beispielsweise eine hybride Intervention seitens Staat B durch Fake-News oder Cyberangriffe nahezu unbeschadet und unbeeindruckt – ohne nennenswerte Kosten – übersteht, reduziert dies drastisch die Wahrscheinlichkeit eines zweiten, ähnlich gearteten Angriffs. Um diesen Ansatz zu implementieren, müssten Staaten ihre Anstrengungen darauf konzentrieren, eine gesamtstaatliche, alle kritischen Bereiche umfassende Widerstands- und Absorptionsfähigkeit aufzubauen, um so gegen Angriffe und Disruption resilienter zu werden.

Auch solche Gedankenspiele sind nicht frei von analytischen und praktischen Fallstricken, da im oben genannten Beispiel ein Angriff eventuell kaum als solcher registriert werden könnte und, wenn doch, dann mitunter auch nur schwer einem bestimmten Akteur zugeordnet werden kann. Auch hier begegnen wir also dem Attributionsproblem – allerdings in entschärfter Form, denn da im Rahmen einer Resilienzstrategie keine Vergeltungsdrohung ausgesprochen würde, könnten fehlende Attributionsmöglichkeiten auch nicht deren Glaubwürdigkeit unterminieren. Identität und Intention des Angreifers wären, zumindest fürs erste, gleichgültig, so lange er denn kräftig entmutigt und von erneuten Anläufen abgeschreckt würde. Mit anderen Worten: Die Resilienzstrategie selbst ist, etwa mit Blick auf den Cyberraum, resilienter als eine Abschreckungsstrategie.

Das Konzept der Abschreckung – insbesondere seine nukleare Dimension – birgt Risiken, bleibt aber weltweit strategisch fest verankert. Nicht jedes neue Phänomen der Sicherheitspolitik kann – und sollte – mit Abschreckung adressiert werden. Aber Abschreckungstheorie und die von der Wissenschaft gewonnenen Erkenntnisse ihrer Anwendung in der Praxis, können als Impuls dienen für neue, der Komplexität der heutigen sicherheitspolitischen Herausforderungen angemessenen strategischen Überlegungen.

1 Siehe „Sicherheitspolitische Dimensionen der Weltraumnutzung", Metis Studie Nr. 13 (August 2019).

Metis

IMPRESSUM

Herausgeber

Metis Institut
für Strategie und Vorausschau
Universität der Bundeswehr
München
metis.unibw.de

Autor

Dr. Konstantinos Tsetsos
metis@unibw.de

Creative Director

Christoph Ph. Nick, M. A.
c-studios.net

Bildnachweis

Titel: Grafik von ndul auf 123RF
S. 4/5: Photo von USAMHI auf wikimedia

ISSN-2627–0587