Hybride Bedrohungen – eine Taxonomie

Der Begriff der hybriden Bedrohung ist in der sicherheitspolitischen Debatte allgegenwärtig, da sich damit ein wenig fassbares Feld unterschiedlicher Angriffstypen zusammenfassen lässt. Diese Analyse argumentiert, dass die zielführende Auseinandersetzung mit einer hybriden Bedrohungslage zunächst ein klares Verständnis der zugrundeliegenden hybriden Formen der Konfliktführung voraussetzt.

Von Ivo Capaul

Die Besatzung der «Yi Peng 3» wird Ende 2024 verdächtigt, zwei Unterseekabel im Baltischen Meer beschädigt zu haben. Abstreitbarkeit ist ein Kernmerkmal hybrider Angriffe. *Mikkel Berg Pedersen / Reuters*

Westliche Staaten sehen sich vermehrt Angriffen ausgesetzt, die in einer Grauzone zwischen Krieg und Frieden zu verorten sind. Dieser Trend hat sich mit dem Ausbruch eines konventionellen Krieges auf dem europäischen Kontinent akzentuiert. Um dieses Phänomen, welches in den letzten Jahren massgeblich zu einer Destabilisierung der Sicherheitslage in Europa beigetragen hat, zu beschreiben, setzt sich momentan der Begriff der hybriden Bedrohung durch. So werden Fallbeispiele wie die Steuerung irregulärer Migrationsbewegungen durch Belarus, die durch chinesische Akteure in sozialen Medien verbreitete Theorie, wonach der COVID-19-Virus einem US-amerikanischen Armee-Versuchslabor entstamme, die Kompromittierung der Systeme von Betreibern kritischer Infrastruktuen und das Leaken einer durch nachrichtendienstliche Mittel abgefangenen Telekonferenz hochrangiger deutscher Offiziere durch russische Behörden als Beweise dafür herangezogen, dass zwischenstaatliche Auseinandersetzungen vermehrt mittels hybrider Konfliktführung ausgetragen werden.

Entsprechend ist im sicherheitspolitischen Diskurs von einem Zeitalter der hybriden Kriegsführung, gar von einer weaponisation of everything die Rede. Diese Entwicklung macht auch vor der Schweiz nicht halt: Der Begriff der *hybriden Bedrohung* hat in den vergangenen Jahren Einzug in zahlreiche sicherheitspolitische Dokumente des Bundes gehalten. Insbesondere orientiert sich eines der vier Szenarien, welche die Schweizer Armee für ihre Streitkräfteentwicklung berücksichtigt, explizit an hybriden Formen der Konfliktaustragung. Gerade aufgrund dieser sich vollziehenden Institutionalisierung ist es notwendig, ein grundlegendes Verständnis davon zu schaffen, was mit «hybrid» gemeint ist und wie dieser Begriff zum Verständnis einer Bedrohungslage beitragen kann.

Ziel der vorliegenden Analyse ist, den Begriff der von Staaten ausgehenden hybriden Bedrohung in dem Sinne zu schärfen, dass ein auf bestehenden Begrifflichkeiten basierender Minimalkonsens an definitorischen Elementen geschaffen werden kann. Die Grundidee dieses Definitionsansatzes ist, dass zur Erfassung einer *hybriden Bedrohungslage* aus der Perspektive des Angegriffenen zunächst ein klares Verständnis der durch den Angreifer verwendeten

hybriden Formen der Konfliktaustragung bestehen muss. Hierzu werden zuerst verschiedene Definitionen sowie die Kritik am Begriff erörtert, bevor eine Taxonomie zur Kategorisierung hybrider Bedrohungslagen vorgestellt wird. Thematisiert werden ebenfalls ein alternativer Ansatz zur Auseinandersetzung mit der Thematik sowie abschliessend die Rolle eines hybriden Bedrohungsbildes als Ausgangspunkt eines Strategieschöpfungsprozesses.

Ein (zu) weites Feld

Zunächst ist festzustellen, dass eine universell anerkannte Definition des Begriffs der hybriden Bedrohung nicht existiert. Das Reglement Operative Führung 17 der Schweizer Armee grenzt den Begriff der von Staaten ausgehenden hybriden Konfliktaustragung als eine Kombination politischer, wirtschaftlicher, informationeller, humanitärer und paramilitärischer Instrumente zur Erreichung strategischer Ziele ein, deren Einsatz in der Regel irregulär und verdeckt erfolgt. Die NATO definiert *hybride Bedrohung* als «eine Art von Bedrohung, die konventionelle, irreguläre und asymmetrische Aktivitäten in Zeit und Raum kombiniert».

Eine universell anerkannte Definition des Begriffs der hybriden Bedrohung existiert nicht.

Im Wesentlichen deckungsgleich ist die Definition der EU, die von einer «Mischung von Zwang und Unterwanderung und von konventionellen und unkonventionellen Methoden (…), auf die von staatlichen oder nichtstaatlichen Akteuren in koordinierter Weise zur Erreichung bestimmter Ziele zurückgegriffen werden kann, ohne dass jedoch die Schwelle eines offiziell erklärten Kriegs erreicht wird», ausgeht. Ähnlich wird das Phänomen in wissenschaftlichen Kreisen charakterisiert; etwa von Reichborn-Kjennerud und Cullen, welche hybride Kriegsführung als gleichzeitige Eskalation in der horizontalen Ebene (Ausweitung feindseliger Aktionen auf alle militärischen und nicht-militärischen Mittel der Staatsgewalt) als auch in der vertikalen Ebene (Intensivierung, nicht nur der Aktionen selber, sondern auch der Koordination von Aktionen in verschiedenen Wirkungsräumen) begreifen.

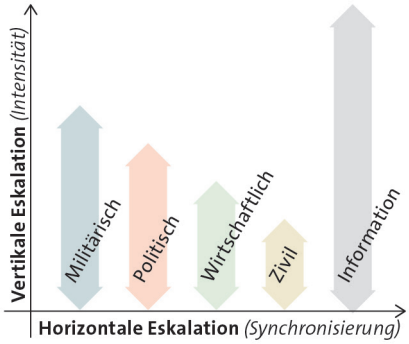
Wie diesen Definitionen zu entnehmen ist, beinhaltet der Begriff der hybriden Bedrohung ein hohes Mass an Abstraktion. Aufgrund dessen hat sich der Begriff zu einer zunehmend unbestimmten Sammelbezeichnung für unterschiedlichste Formen der Bedrohung durch nonlineare Konfliktführung entwickelt. So wurde etwa eine öffentliche Äusserung des russischen Aussenministers Sergej Lawrow als eine Form hybrider Kriegsführung bezeichnet, genauso wie die Besetzung und anschliessende Annexion der Krim durch nicht gekennzeichnete russische Soldaten im Jahr 2014 («kleine grüne Männchen»). Die Spannbreite zwischen diesen zwei Beispielen verdeutlicht, dass die hybride Bedrohung eine zu inklusive Begrifflichkeit darstellt, um trennscharf eine Ausprägung der Konfliktführung von anderen abgrenzen zu können.

Ein weiterer Kritikpunkt besteht darin, dass der Begriff der hybriden Konfliktführung im Kern kein neues Phänomen beschreibt, sondern lediglich eine neue Bezeichnung für eine historisch gewachsene Praxis darstellt. Die Tendenz von Staaten, ihre Interessen gegenüber anderen Staaten auch mithilfe subversiver Mittel und unterhalb der Kriegsschwelle durchzusetzen, ist wohl ebenso alt wie zwischenstaatliche Konflikte an sich. Bereits aus den Schriften Sun Tsus lässt sich ein entsprechendes Verständnis der Kriegskunst herauslesen. Gleichwohl wird aus der gegenwärtigen Popularität des Begriffs klar, dass es sich bei hybrider Konfliktführung um ein Bedrohungsbild handelt, mit welchem sich politische und militärische Entscheidungsträger gerade in westlichen Staaten zunehmend stark auseinandersetzen.

Dieses verstärkte Interesse lässt sich durch zwei wesentliche Entwicklungen erklären. Einerseits hat sich, bedingt durch die Verbreitung neuer Technologien wie den sozialen Medien, der Wirkungsraum subversiver Massnahmen ausgeweitet. Andererseits zeigt sich, dass subversive Angriffe insbesondere dann für Staaten zu einem attraktiven Machtmittel unterhalb der Kriegsschwelle werden, wenn die potenziellen Kosten einer Konflikteskalation nicht tragbar wären – insbesondere unter Bedingungen der nuklearen *Mutually Assured Destruction* ist dies der Fall. Aus diesem Grund waren Angriffe, welche man heutzutage als *hybrid* designieren würde, während des Kalten Krieges weit verbreitet (oft als *Aktive Massnahmen* oder *Covert Action* bezeichnet) und können heutzutage, in einer Zeit zunehmender geopolitischer Polarisierung, wieder vermehrt aufkommen.

Hybride Kriegsführung

Gemäss der Definition von Reichborn-Kjennerud und Cullen



Während der Begriff der hybriden Bedrohung also eine relevante Kategorie des gegenwärtigen sicherheitspolitischen Diskurses darstellt – was sich auch in seiner zunehmenden Verankerung in den Strategiedokumenten des VBS, der NATO und der EU niederschlägt – besteht die Gefahr, dass er zu einer inhaltslosen Begriffshülse verkommt. Können nämlich alle Arten von zwischenstaatlichen Auseinandersetzungen, die keine konventionellen Kriege sind, als *hybrid* bezeichnet werden, dann ist dieser Begriff zu umfassend und gleichzeitig zu vage, um einen sinnvollen Beitrag zum Verständnis einer Bedrohungslage darzustellen.

Fokus auf Angriffsvektoren

Eine Möglichkeit, mehr Klarheit in den diffusen Begriff der hybriden Bedrohung zu bringen, besteht in einem Perspektivenwechsel: Weg von einer Bedrohungswahrnehmung aus Sicht des hybrid Angegriffenen, hin zur Betrachtung der von einem Aggressor ausgehenden Angriffsvektoren, die dem Spektrum der hybriden Konfliktführung zuzuordnen sind. Hybride Angriffe sind die einzigen empirisch beobachtbaren Elemente in der Debatte um hybride Konfliktführung und können folglich als Ausgangspunkt einer induktiv ausgerichteten Analyse eines hybriden Gefahrenbildes dienen. Erst die Analyse bereits stattgefundener und als hybrid klassifizierbarer Angriffe ermöglicht es – in Kombination mit der Extrapolation zukünftig möglicher Angriffe – ein Lagebild hybrider Bedrohungen auch wirklich mit Inhalt zu füllen.

Ein «Angriff» ist die Ergreifung offensiver Massnahmen gegen ein bestimmtes Ziel. Ein Angriff geht also von einem Akteur aus

und richtet sich gegen einen anderen Akteur. Daraus folgt, dass ein von einem Staat durchgeführter hybrider Angriff drei grundlegende Definitionselemente aufweisen muss: Erstens, einen Aggressor, der durch den Angriff einen Effekt erzielen will; zweitens, einen Angegriffenen (staatliche Institution, Zivilbevölkerung etc.), auf welchen eine Wirkung erzielt werden soll; sowie, drittens, einen hybriden Angriffsvektor. Dieser Vektor stellt die eigentliche offensive Massnahme dar und verbindet Aggressor und Angegriffenen miteinander (siehe Abbildung).

Modell zur Beschreibung hybrider Angriffe

Quelle: Eigene Darstellung

Die Charakteristiken dieses Vektors sind dann auch diejenigen Elemente, welche einen Angriff erst *hybrid* werden lassen. Um als hybrid klassifiziert zu werden, muss der Angriffsvektor drei Eigenschaften aufweisen; er muss erstens, ein Mass an *Abstreitbarkeit (plausible deniability)* aufweisen; zweitens, *asymmetrisch* sein; und drittens, in seiner *Intensität* unterhalb der Kriegsschwelle liegen. Diese drei Kriterien, welche den Definitionen der hybriden Bedrohung der Schweizer Armee und der EU entstammen, bedürfen einer Erläuterung.

Abstreitbarkeit beschreibt den Grad, zu dem der hybrid angreifende Staat beziehungsweise dessen politische Führung glaubhaft abstreiten kann, Urheber des Angriffs zu sein. Sofern dies gegeben ist, reduzieren sich die politischen Kosten, die für den Aggressor in Kauf zu nehmen sind, indem etwa Vergeltungsmassnahmen des Angegriffenen (beispielsweise in Form von Sanktionen) weniger wahrscheinlich werden. Aus diesem Grund finden hybride Angriffe oft unter Zuhilfenahme nachrichtendienstlicher Vorgehensweisen statt – also verdeckt (Urheber bleibt verborgen) oder gar klandestin (Angriff als solcher bleibt verborgen).

Asymmetrie bezieht sich auf den Wirkungsraum, in welchem der hybride Angriff durchgeführt wird (soziale Medien, Wirtschaft, Zivilgesellschaft etc.). Ein Angriffsvektor wird dadurch asymmetrisch, indem er in denjenigen Wirkungsräumen ansetzt, in welchen der Angegriffene unzureichende Abwehrdispositive besitzt. Im Grunde genommen handelt es sich bei diesem Verständnis von Asymmetrie um eine Ausnützung der relativen Stärken des Aggressors gegenüber den Schwächen des Angegriffenen. Ein typischer hybrider Angriffsvektor ist beispielsweise die vorsätzliche Streuung von Desinformation. In offenen, demokratischen Gesellschaften besitzt das Gut der Meinungs- und Informationsfreiheit einen hohen Stellenwert, weshalb staatlichem Handeln zur Bekämpfung von Desinformation oft enge Grenzen gesetzt sind.

Schliesslich adressiert die *Intensität* des Angriffsvektors das Eskalationspotenzial eines hybriden Angriffs im Verhältnis zur konventionellen Konfliktführung. Ein hybrider Angriffsvektor ist hinsichtlich der Intensität seiner Wirkung auf den Angegriffenen in einem Mass dosiert, sodass er sich auf der Eskalationsleiter unterhalb der Kriegsschwelle befindet. Ist ein hybrider Angriff derart intensiv, dass sich der angegriffene Staat gezwungen sieht, mit seinen Streitkräften konventionell dagegen vorzugehen, so ist die Kriegsschwelle überschritten. Ein Anzeichen, dass sich ein Angriff der Kriegsschwelle annähert, besteht darin, dass ein ansonsten als hybrid zu bezeichnender Angriffsvektor auch eine kinetische Dimension besitzt. In einem solchen Fall kann von einem Konflikt in der *Grey Zone* gesprochen werden.

> Erst die Analyse als hybrid klassifizierbarer Angriffe ermöglicht es ein Lagebild hybrider Bedrohungen auch wirklich mit Inhalt zu füllen.

Beispielhaft für Angriffe in der *Grey Zone* steht die Art und Weise, wie der Konflikt im Donbas von russischer Seite zwischen 2014 und 2022 geführt wurde, also unter Zuhilfenahme paramilitärischer Einheiten, Cyberangriffen und Desinformation. Relevant ist ebenfalls, dass die Intensität eines Angriffsvektors sich invers zum Faktor der Abstreitbarkeit verhält. Je höher die Intensität eines hybriden Angriffsvektors, desto niedriger ist tendenziell seine Abstreitbarkeit.

Weist ein Angriffsvektor diese drei Charakteristiken auf, so kann im Sinne der vorliegenden Definition von einem hybriden Angriff gesprochen werden. Ein Staat, dessen Interessen realistischerweise durch solche Angriffsvektoren tangiert werden, sieht sich mit einer hybriden Bedrohungslage konfrontiert.

Klassifizierung der Bedrohungslage

Zentral für diesen Definitionsansatz ist, dass es sich bei den ihm zugrunde liegenden drei Kriterien nicht um binäre Variablen handelt. Diese sind nicht einfach vorhanden oder nicht vorhanden, sondern verlaufen auf einem Spektrum. Die Beurteilung des Ausmasses, zu welchem diese Kriterien verwirklicht sind, ermöglicht dadurch eine Klassifizierung von drei unterschiedlichen hybriden Bedrohungslagen (siehe Tabelle). Die in dieser Klassifizierung verwendete Terminologie stimmt mit jener der EU überein.

Weiterhin kann eine solche Klassifizierung zur Klärung der Zuständigkeiten zwischen denjenigen staatlichen Akteuren dienen, die für die Abwehr von Angriffen in den drei in der Tabelle dargestellten Bedrohungslagen hauptsächlich verantwortlich sind. Beispielsweise sind Identifizierung und Abwehr hybrider Operationen primär nachrichtendienstliche Aufgaben, während die Armee voraussichtlich erst bei der Schwelle zur hybriden Kriegsführung eine führende Rolle einnimmt.

Ein alternativer Ansatz

Ein alternativer Ansatz zur Entwirrung des Konzepts hybrider Bedrohungen kann darin bestehen, dieses in zahlreiche Unterkategorien aufzuspalten. Dabei wird dem Begriff der hybriden Bedrohung seine Ausdruckskraft abgesprochen. Die Auseinandersetzung mit den hier als hybrid bezeichneten Angriffen findet innerhalb des jeweiligen Wirkungsraums statt, in welchem sich ein Angriffsvektor entfaltet. Einzelne Angriffe werden in diesem Ansatz nicht als zusammenhängende Phänomene betrachtet und als solche auch getrennt voneinander analysiert.

Kategorisierung hybrider Bedrohungslagen gemäss den Definitionskriterien des hybriden Angriffsvektors

Bezeichnung	Abstreitbarkeit	Asymmetrie	Intensität	Beispiele
Hybride Einmischung	Hoch: *«plausible deniability»*	Stark asymmetrisch	Unterhalb der Kriegsschwelle	Desinformation über soziale Medien
Hybride Operationen	Mittel: *«rather plausible deniability»*	asymmetrisch	Unterhalb der Kriegsschwelle	Sabotage kritischer Infrastruktur
Hybride Kriegsführung	Tief: *«implausible deniability»*	paramilitärisch	Konflikte in der *«Gray Zone»* (nahe der Kreigsschwelle)	Kleine grüne Männchen, absichtlich erzeugte Flüchtlingsbewegungen
Konventioneller Krieg	Nicht vorhanden	militärisch (symmetrische Kriegsführung)	Kriegsschwelle überschritten	Russische Vollinvasion der Ukraine seit 2022

Eigene Darstellung in terminologischer Anlehnung an Wigell, Mikkola und Juntunen.

Der Vorteil dieses Ansatzes ist es, dass damit präziser eingrenzbare Kategorien entstehen, was eine detailliertere Analyse von Angriffsvektoren innerhalb ihrer jeweiligen Wirkungsräume ermöglicht. Gleichzeitig sind mit dieser Vorgehensweise aber mindestens zwei Nachteile verbunden. Erstens liegt es in der Natur hybrider Angriffe, dass sich deren Wirkung über mehrere überlappende Wirkungsräume entfaltet. So findet eine Desinformationskampagne über das Internet sowohl im Cyber- als auch im Informationsraum statt, wodurch die Untersuchung eines solchen Angriffs innerhalb nur eines Wirkungsraums zu kurz gedacht wäre. Zweitens versucht der Begriff der hybriden Konfliktführung explizit eine integrative, mehrere Wirkungsräume umfassende Strategie eines Angreifers abzubilden.

Durch die Aufspaltung des hybriden Begriffs in einzelne Domänen ginge eben jenes Kernelement des Hybriden, im Sinne eines Verbunds an Angriffsvektoren zur Erreichung einer Wirkung gegenüber dem Angegriffenen, verloren. Relevant ist eine solche integrative Sichtweise des Bedrohungsbildes insbesondere für die Abwehr von hybriden Angriffen, weil dazu voraussichtlich die Koordination der verschiedenen sicherheitspolitischen Instrumente eines Staates benötigt wird. Folglich ist eine Zerstückelung des Begriffs der hybriden Bedrohung in seine Wirkungsräume auf der strategischen Ebene – auf welcher sich diese Analyse bewegt – abzulehnen. Hier steht der integrierte Charakter hybrider Bedrohungen im Vordergrund. Auf der Ebene der operationellen Gefahrenabwehr hingegen kann eine Unterteilung der Bedrohungen in unterschiedliche Wirkungsräume durchaus sinnvoll sein, da sich dadurch klären lässt, welche staatliche Institution für die Durchführung von Gegenmassnahmen zuständig ist.

Grundlage zur Strategieschöpfung

Der Begriff der hybriden Bedrohung ist in der sicherheitspolitischen Debatte allgegenwärtig, weil sich damit ein wenig fassbares Feld unterschiedlicher Angriffstypen mit einem Schlagwort zusammenfassen lässt. Gleichzeitig bewirkt dieser Umstand, dass der Definitionsraum des Begriffs zunehmend ausgeweitet wird. Dadurch kommt diesem die Trennschärfe abhanden. Eine Lösung dieser Problematik kann darin bestehen, ein hybrides Bedrohungsbild basierend auf den abstrakten Eigenschaften derjenigen Angriffsvektoren zu definieren, welche als «hybrid» eingeordnet werden können.

Um eine solche Klassifikation durchführen zu können, schlägt diese Analyse –basierend auf den Terminologien der Schweizer Armee, der NATO und der EU – die drei Kriterien *Abstreitbarkeit, Asymmetrie* und *Intensität* vor. Die Ausprägung dieser drei Kriterien kann als Referenzrahmen zur Schaffung eines Lagebilds hybrider Bedrohungen dienen. Darüber hinaus trägt dieser Ansatz dazu bei, die Beurteilung einer hybriden Bedrohungslage besser in der empirischen Realität zu verankern. Zur Vervollständigung einer Bedrohungsbeurteilung nach diesem Verfahren wäre darüber hinaus eine Analyse der konkreten Ziele notwendig, welche durch den Aggressor bei einem hybriden Angriff verfolgt werden. Dieser Aspekt wurde in dieser Analyse nicht berücksichtigt.

Abschliessend gilt es zu betonen, dass es sich beim Begriff der hybriden Bedrohung um eine Orientierungshilfe handelt, die dazu dient, ein empirisch beobachtbares Bedrohungsbild erfassen und kategorisieren zu können. Was der Begriff aber dezidiert nicht darstellt, ist eine Strategie im Sinne einer Konzeption, wie die Instrumente eines Staates eingesetzt werden können, um aus Sicht des Angegriffenen auf hybride Bedrohungen zu reagieren. Dies wäre ein nachgelagerter Schritt, welcher voraussichtlich nach einem gesamtstaatlich integrativen (*whole-of-government*-, beziehungsweise *whole-of-society*-) Ansatz verlangt. Um eine solche Strategie formulieren zu können, ist es zunächst in einem vorgelagerten Schritt notwendig, ein klares Verständnis für das konkret vorliegende hybride Bedrohungsbild zu schaffen.

Für mehr zu Verteidigungspolitik und Rüstungsbeschaffung, siehe CSS Themenseite.

Ivo Capaul ist Researcher im Team Verteidigungspolitik und Rüstungsbeschaffung am Center for Security Studies (CSS) der ETH Zürich.

Die **CSS Analysen zur Sicherheitspolitik** werden herausgegeben vom Center for Security Studies (CSS) der ETH Zürich. Das CSS ist ein Kompetenzzentrum für schweizerische und internationale Sicherheitspolitik. Jeden Monat erscheinen zwei Analysen auf Deutsch, Französisch und Englisch.

Herausgeber: Lucas Renaud
Lektorat: Lucas Renaud, Amos Dossi
Layout und Grafiken: Miriam Dahinden-Ganzoni

Feedback und Kommentare: css.info@sipo.gess.ethz.ch
Weitere Ausgaben und Abonnement: www.css.ethz.ch/cssanalysen

ISSN: 2296-0236; DOI: 10.3929/ethz-b-000709033