

Die unsichtbare Front Informationshoheit, Abschreckung, Resilienz: So heißen die wichtigsten Verteidigungslinien gegen hybride Kriegsführung. Deutschland hat hier erheblichen Nachholbedarf.

Von Jan Stöckmann

Anfang Juli, auf der Ostsee vor Fehmarn. Etwa 15 Kilometer vom Strand entfernt passiert der Öltanker Kira K. die Meerenge zwischen Dänemark und Deutschland. Er wird der russischen Schattenflotte zugerechnet, die bis zu 1400 solcher Schiffe umfasst; viele von ihnen sind marode. Offiziell fährt der Tanker unter der Flagge Panamas, aber die Eigentumsverhältnisse sind unklar, wie so oft bei Schiffen dieser Art. Bisweilen wechseln sie ihre Namen und Beflaggung auf offener See. Russlands Ziel: westliche Sanktionen umgehen, um mit dem Ölgeschäft von geschätzt 85 Milliarden Dollar jährlich die Kriegskasse zu füllen.

An diesem Tag fährt eine Gruppe von Umweltschützern, Abgeordneten und Journalisten auf Schlauchbooten in die Nähe der Kira K., um auf die Umwelt- und Sicherheitsgefahren dieser Schiffe aufmerksam zu machen. Mit dabei sind die Bundestagsabgeordneten Robin Wagener von den Grünen und Thomas Röwekamp von der CDU sowie der schwedische Europaabgeordnete Jonas Sjöstedt und mehrere Greenpeace-Aktivisten. Plötzlich

taucht ein russisches Kriegsschiff auf und fährt mit hoher Geschwindigkeit auf die Schlauchboote zu. Die Situation droht zu eskalieren. Über Funk von der ebenfalls herbeigeeilten deutschen Küstenwache zur Rede gestellt, bleiben die Russen vage. Sie sprechen von „besonderen Plänen“ und eskortieren den Tanker schließlich durch den Fehmarnbelt.

Schattentanker im Visier

Dass die Kira K. an der deutschen Küste vorbeifährt, statt den kürzeren Weg durch schwedische Gewässer zu wählen, hat einen Grund. Denn Schweden geht härter gegen die Schattenflotte vor. Auch Großbritannien, Frankreich und die USA nehmen Schattentanker ins Visier. Damit bringen sie Russland so weit in Bedrängnis, dass Moskau sich veranlasst sieht, zumindest einige Schiffe offiziell unter russischer Flagge zu registrieren, so auch die Kira K. Seit August 2026 trägt das nun russische Schiff den Namen Khrizolit.

Doch damit ist es nicht getan. Angreifer wie Russland suchen stets neue Schwachstellen. Ihr Vorgehen hat System – ein



Dr. Jan Stöckmann
ist Leiter des Karl
Kaiser Forums
für strategische
Fragen der DGAP.

System, das man nicht mehr als Kette von Einzelfällen betrachten kann, sondern als hybriden Krieg bezeichnen muss. Mit dem bewaffneten Drohnenangriff am Flughafen Leipzig/Halle Anfang August hat Russland abermals eskaliert. Auch für Berlin ist mittlerweile klar: So kann es nicht weitergehen. Deutschland befindet sich zwar nicht im Krieg, so Außenminister Johann Wadephul, doch „russisches Kriegsziel“ sei man schon. Was bedeutet das?

Krieg ist, mit Clausewitz gesprochen, die Fortsetzung der Politik mit anderen Mitteln. Genau das geschieht, wenn der Kreml mit Drohnen und Propaganda die deutsche Gesellschaft zu untergraben versucht; wenn er rechtswidrig und teils gewaltsam Sanktionen umgeht. In gewisser Weise haben Kriegsparteien schon immer auf nichtkinetische Waffen zurückgegriffen. Neu sind die Professionalität und die Intensität, mit der Staaten hybride Mittel einsetzen. Staatlich unterstützte Kriminalität wird zum Normalzustand. Seit 2025 bietet die Moskauer Wirtschaftshochschule einen Masterstudiengang in Sanktionsumgehung an.

Die Tanker der russischen Schattenflotte sind Teil dieses Krieges gegen Deutschland und seine Verbündeten. Sie unterwandern internationales See- und Handelsrecht, finanzieren den Angriffskrieg gegen die Ukraine und gefährden die Umwelt. Es gibt zudem Anzeichen, dass Schattentanker als schwimmende Plattformen für Spionage und Drohnen-

angriffe genutzt werden könnten. Es wird Zeit, diesen Krieg besser zu verstehen und systematischer zu bekämpfen.

Der Vorfall bei Fehmarn legt drei Kernmerkmale hybrider Kriegsführung exemplarisch offen. Erstens: Die Angreifer verschleiern ihre Identität, in diesem Fall durch die irreführende Beflaggung von Handelsschiffen, stehen aber letztlich unter der Kontrolle staatlicher Akteure. Das betrifft etwa autoritäre Staaten wie Russland, den Iran oder China; die Grenzen zwischen offizieller Politik und finanziell motivierter Kriminalität sind dabei nicht immer trennscharf. Die Unkenntlichmachung erschwert es rechtsstaatlichen Behörden, schnell zu reagieren, was die Angreifer natürlich einkalkulieren.

Zweitens: Die Angriffe umfassen ein Bündel von Mitteln und Methoden, darunter sowohl ökonomische, diplomatische, technologische und informationelle als auch konventionell militärische. Im Fall der Kira K. trat das russische Kriegsschiff als Untermauerung der ökonomischen Kriegsführung auf, also der Umgehung internationaler Sanktionen. Hinzu kommt das Spiel mit Umweltbedrohungen, denn viele Schiffe der Schattenflotte sind alt und schlecht gewartet: Im Januar 2025 trieb ein anderer mutmaßlicher Schattentanker, die Eventin, manövrierunfähig vor Rügen.

Schließlich zeichnet sich hybride Kriegsführung dadurch aus, dass sie nicht auf den schnellen Triumph oder die militärische Eskalation abzielt, sondern auf die sukzessive Schwächung gesellschaftlicher Stabilität und politischer Handlungsfähigkeit. Das Vorgehen des russischen Kriegsschiffs im Fall der Kira K. galt nicht in erster Linie den Schlauchbooten oder ihren Passagieren, sondern der Einschüchterung und dem Ausbremsen von gesellschaftlichem und politischem

*Seit 2025 bietet die
Moskauer Wirtschaftshochschule einen
Masterstudiengang in
Sanktionsumgehung an*

Engagement. Oft werden Angriffe zudem mit gezielter Desinformation gepaart und der Westen als eigentlicher Aggressor dargestellt, um eine Rechtfertigung zu konstruieren und um Zweifel im öffentlichen Diskurs zu sähen. Mit anderen Worten: Hybride Angreifer nehmen besonders schwer zu schützende Ziele ins Visier.

Aus diesen drei Merkmalen hybrider Kriegsführung – ihrer Akteure, Methoden und Ziele – lassen sich Ansatzpunkte für hybride Verteidigung entwickeln, ähnlich wie in den 1940/50er Jahren die Grundlagen nuklearer Abschreckungstheorie entstanden sind. Damals waren es Atomwaffen, die die Logik von Konflikten revolutionierten und die Parameter wirksamer Verteidigung verschoben. Heute sind es die Spezifika hybrider Angriffe, die uns zwingen, alte Schablonen zu überdenken.

Die Angriffe einfach hinzunehmen, würde nur zu weiteren einladen. Auch das Einbestellen von Botschaftern hat kaum mehr als eine symbolische Bedeutung. Nur wenn die Angreifer damit rechnen müssen, dass ihnen selbst Kosten entstehen – und wenn die Erfolgswahrscheinlichkeit in einem negativen Verhältnis zum Aufwand steht –, werden sie von ihrem Tun ablassen. Für Deutschland wiederum heißt das: Hybride Verteidigung muss erstens gut informiert sein, zweitens sorgfältig ausgewählte Gegenmaßnahmen zur Abschreckung bereithalten und drittens gesamtgesellschaftliche Resilienz aufbauen.

Strategische Ambiguität

Die Verschleierungstaktik hybrider Angreifer macht es wichtig, schnell und präzise aufzuklären. Es kann nicht sein, dass die Ausflagung von Handelsschiffen in Offshore-Registern zu langsamerer Verfolgung von Regelverstößen führt. Auch die Identifikation von Drohnenüberflügen

dauert zu lange. Das führt zu einer diffusen Nachrichtenlage, in der sich irreführende Narrative leicht durchsetzen. Der Verschleierungstaktik der Angreifer muss Deutschland mit eigener Informationshoheit begegnen.

Wie das geht? Nachrichtendienstliche Fähigkeiten aufbauen, behördliche Vernetzung verbessern, wirtschaftliche Schäden beziffern, überzeugende Informationskampagnen starten – das wäre ein Anfang. Es ist bezeichnend, dass die 2025 veröffentlichte Broschüre des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe (BBK) nicht an Haushalte verschickt wurde, weil man offensichtlich befürchtete, der Bundesregierung fehle die notwendige Glaubwürdigkeit.

Aus dem zweiten Merkmal, dem frei gewählten Einsatz konventioneller und nichtkonventioneller Mittel, ergibt sich die gebotene Antwort: Abschreckung durch asymmetrische Gegenmaßnahmen. Schon aus völkerrechtlichen Gründen verbietet es sich, auf einen Krankenhaus-Hackerangriff mit gleichen Mitteln zu antworten oder den russischen Ölschmuggel mit dem Aufbau einer eigenen Schattenflotte zu erwidern.

Aber auch in strategischer Hinsicht liegt ein Vorteil in asymmetrischen Reaktionen. Sie ermöglichen es, dosiert vorzugehen und dem Aggressor schwer kalkulierbare Kosten aufzuerlegen: die sogenannte strategische Ambiguität. Außerdem lassen sich so Eskalationsrisiken besser kontrollieren und die eigene

*Nur wenn die Angreifer
mit hohen Kosten rechnen
müssen, werden sie von
ihrem Tun ablassen*

Trügerischer Glanz: Der Tanker Kira K. gehört zur russischen Schattenflotte. Mit Hilfe dieser Flotte will Moskau westliche Sanktionen umgehen, um mit dem Ölgeschäft die Kriegskasse zu füllen.

Zuordenbarkeit steuern. Ein gutes Beispiel ist der sogenannte Hackback, also die digitale Verfolgung von Hinterleuten und die Beschlagnahmung von Vermögenswerten. Im Fall der Schattenflotte hieße das neben rigorosem Eingreifen auf See die Verfolgung und Sanktionierung russischer Oligarchen und anderer Profiteure des illegalen Geschäfts.

Drittens: Um die Angriffe auf unsere Gesellschaft abzufedern, braucht es Resilienz in Politik, Wirtschaft und Gesellschaft. Man kann nicht jede Stromtrasse lückenlos schützen. Aber je dichter das Netz aus Resilienzmaßnahmen ist, desto geringer sind die Erfolgschancen für die Angreifer und desto höher die Kosten pro erfolgreichen Angriff.

Umgekehrt gebietet eine nüchterne Kosten-Nutzen-Analyse, auf der Verteidigungsseite ebenfalls zu priorisieren und da zu investieren, wo zusätzliche Resilienz den größten Effekt hat. So werden in Schweden Sensibilisierungs- und Ausbildungsmaßnahmen von oben nach unten ausgerollt, statt die gesamte Bevölkerung auf einmal zu erreichen. Warum, fragt man sich, wird kritische Infrastruktur wie Transportwege oder die Stromversorgung immer noch nicht ausreichend geschützt? Gäbe es bei Havarie eines russischen Schattentankers ausreichend Personal und Material für den Küstenschutz? Wer entscheidet politisch über das Kritischste der kritischen Infrastruktur?

Restriktive Abschreckung

Natürlich wird man in keiner der drei Dimensionen Perfektion erreichen. Nicht jeder Angriff wird sich zweifelsfrei zuord-

nen lassen. Die Androhung von Gegenmaßnahmen wird nicht jede Aggression abschrecken. Und auch die Resilienzvorkehrungen werden nicht alle Verwundbarkeiten schützen können. Die Idee hybrider Verteidigung ist nicht absolute Abschreckung wie im Kalten Krieg, sondern restriktive Abschreckung, wie Experten des Hybrid Center of Excellence in Helsinki argumentieren. Diese Abschreckung versucht nicht jeden Angriff abzuwehren, aber doch ihre Zahl und Schwere deutlich zu reduzieren. Letztlich ist hybrider Krieg eine Ressourcenfrage, wie jeder Krieg.

Ein weiterer Vorteil restriktiver Abschreckung ist, dass sie keine falsche Sicherheit verspricht, sondern das gesamtgesellschaftliche Handlungsbedürfnis unterstreicht. In der hybriden Welt gibt es viele Stellschrauben in Staat, Wirtschaft und Gesellschaft. Jede IT-Sicher-

Bild nur in
Printausgabe
verfügbar

heitskampagne privater Unternehmen hilft ebenso, Aggressoren abzuschrecken wie zivilgesellschaftliches Engagement gegen vom Ausland induzierten Populismus. Treiber und Taktgeber muss gleichwohl der Staat sein. Nur wenn es klare politische Bereitschaft auf den höchsten Entscheidungsebenen gibt, lassen sich robuste Gegenmaßnahmen umsetzen.

Gelingen kann das nur, wenn die drei Verteidigungslinien – Informationshoheit, Abschreckung, Resilienz – ineinandergreifen. So sollten Behörden früher und umfassender Kenntnis über russische Machenschaften auf der Ostsee haben, um Gegenmaßnahmen starten zu können. Bundeswehr, Grenz- und Küstenschutz sind auf effektive politische Kommunikation angewiesen, damit ihre Fähigkeiten abschreckende Wirkung entfalten, ohne eingesetzt werden zu müssen. Und auch die mächtigste Marine wird nur obsiegen, wenn der Heimathafen gut geschützt und die Matrosen gut ausgebildet sind.

Eine wichtige Voraussetzung hierfür ist das Aufspüren von Finanzströmen, um die Drahtzieher von Angriffen ausfindig zu machen. Bereits heute gibt es hierfür KI-gestützte Lösungen. Hier ließe sich viel von der Terror- und Geldwäschebekämpfung lernen. Denn auch Terroristen, Schmuggler und hybride Angreifer tauschen sich aus. Ob Schattentanker oder Wegwerfagenten: Die Instrumente der Drahtzieher ähneln sich. Um international auf Augenhöhe mitspielen zu können, müssen auch nachrichtendienstliche Fä-

higkeiten erweitert werden. Der BND-Gesetzentwurf hält wichtige Impulse bereit.

Aufrüstung und Befähigung allein werden aber nicht reichen, denn hybride Kriegsführung ist kein statischer Grabenkampf. Die Methoden der Aggressoren entwickeln sich ständig weiter, während das Schaden-Kosten-Verhältnis stetig zunimmt. Schon heute ermöglichen es Bots und Wegwerfagenten, hybriden Krieg zu Discountpreisen zu führen. Es gewinnt, wer am kreativsten und dreistesten ist. Eine Recherche des Organized Crime and Corruption Reporting Project zeigt, dass Crewmitglieder der Schattenflotte Verbindungen zur Wagner-Gruppe oder zu russischen Geheimdiensten haben.

Wie lange wird es dauern, bis Deutschland Antworten auf die nächste und übernächste Generation hybrider Taktiken gefunden haben wird? Warum lässt man es zu, dass die Angreifer immer weiter eskalieren? Die Bundesregierung würde gut daran tun, in Szenarien und Strategiespielen mögliche Angriffsmuster zu antizipieren und ihre Abwehrkräfte entsprechend vorzubereiten. Auch hier sind europäische Partner weiter.

Schließlich lohnt es sich, in landesspezifische Expertise zu investieren, um die Besonderheiten der Angreifer zu verstehen. Denn auch hier dürfte sich künftig einiges verschieben. Während heute Russland für die meisten Angriffe verantwortlich ist, könnten schon bald andere Akteure wie China in den Vordergrund rücken, die noch weitreichendere Ziele verfolgen. Die Unterwanderung unserer wirtschaftlichen und gesellschaftlichen Grundbedingungen dürfte um einiges schwerer abzuwehren sein als ein 250-Meter-Tanker vor der Küste Fehmarns. Der passierte am 22. Juli den Suez-Kanal und nahm Kurs auf Sikka (Indien) – Russlands Lieblingsabnehmer für Rohöl.

IP

*Schon heute ermöglichen
es Bots und Wegwerfagen-
ten, hybriden Krieg zu
Discountpreisen zu führen*