ObstdG Dr. Markus REISNER, PhD

Hybride Kriegsführung

Von grünen Männchen, den fünf Bären, Trollen und Wegwerfagenten

Der Ukraine-Krieg tobt nicht nur auf dem Schlachtfeld. Er findet ebenfalls im Verborgenen statt – inmitten der westlichen Gesellschaft, die zunehmend ins Visier Russlands gerät. Um seine Ziele zu erreichen, nutzt Russland ein breites Instrumentarium im Cyber- und Informationsraum – von Desinformation über Einflussnahme bis hin zu Sabotage und verdeckten Operationen.

In vielen militärischen Beiträgen wird vorrangig das sichtbare Schlachtfeld thematisiert, das in die Domänen Land, See, Luft und Weltraum unterteilt wird. Der Cyberraum, der Informationsraum und das elektromagnetische Feld sind weitere wichtige Domäne. Hybride Kriegsführung findet vor allem im Cyber- und Informationsraum statt. Der Cyberraum ist der „Zauberteppich", auf dem die Informationen aus dem Informationsraum zur Zielgruppe gelangen soll. Im Falle eines hybriden Krieges sind das de facto alle Mitglieder der Gesellschaft eines Staates. Dass der Ukraine-Krieg auf den Domänen Land, See und Luft geführt wird, ist leicht erkennbar. Weniger sichtbar ist, dass Russland im Cyber- und Informationsraum versucht, die Gesellschaften Europas zu beeinflussen. [1]

Hybride Kriegsführung ist eine Form moderner Einsatzführung um militärische, politische, wirtschaftliche und/oder gesellschaftliche Ziele zu erreichen. Dabei werden von staatlichen oder nichtstaatlichen Akteuren reguläre und irreguläre, militärische und zivile, physische und digitale Mittel koordiniert eingesetzt. Ziel dieser offenen und verdeckten Maßnahmen ist das Schwächen eines Gegners, ohne einen klassischen Krieg zu führen. Die Grenze zwischen Krieg und Frieden wird bewusst verwischt, um rechtliche, moralische und politische Reaktionen abzuschwächen oder zu umgehen. [2]

Bekannte Prinzipien und Methoden

Um sich der hybriden Kriegsführung Russlands zu nähern, gilt es zunächst, das unsichtbare Schlachtfeld zu betrachten. Moskau wendet im Prinzip Methoden und Taktiken auf Basis jener Doktrin an, die bereits zu Zeiten der Sowjetunion – auch im Westen – bekannt waren. Damals gab es ein ausgeklügeltes System der Beeinflussung und der Machtprojektion, das im Wesentlichen die vier Bereiche

- **subversive Handlungen (im Informationsraum des angegriffenen Staates)**
- **Stellvertreterhandlungen (im Informationsraum des angegriffenen Staates)**
- **Interventionen (auf dem Hoheitsgebiet des angegriffenen Staates)**

[1] Biermann, K. (2026), *So führen russische Söldner ihren Schattenkrieg gegen Europa, https://www.zeit.de/politik/ausland/2026-02/geheimdienst-gru-russland-soeldner-sabotage-wagner-gruppe*

[2] UK-Parliament (2026), *Disinformation diplomacy: How malign actors are seeking to undermine democracy., https://committees.parliament.uk/work/8818/disinformation-diplomacy-how-malign-actors-are-seeking-to-undermine-democracy/*

- **offensive Handlungen (auf dem Hoheitsgebiet des angegriffenen Staates)**

umfasste und das de facto bis heute aktuell ist, bzw. in Russland gelehrt wird.[3]

In diesem Zusammenhang gilt es, zwischen Maßnahmen im Informationsraum und Maßnahmen, die bereits auf dem Hoheitsgebiet eines Staates stattfanden bzw. stattfinden, zu unterscheiden. Die Sowjets kannten dabei eine Unterteilung in die auf die genannten Bereiche abgestimmten Phasen:

- **Demoralisierung des angegriffenen Staates und seiner Bevölkerung**
- **Destabilisierung (= Spaltung) des angegriffenen Staates und seiner Bevölkerung**
- **Herbeiführung einer Krise (= Handlungsunfähigkeit) im angegriffenen Staat**
- **Militärische Intervention (= Normalisierung) des Angreifers**

Die Demoralisierung kann, so die damalige sowjetische Doktrin, bis zu zehn Jahre dauern. Dies wurde am Beispiel der Ukraine von Russland von 2004 bis 2014 angewandt. Die folgende Destabilisierung eines Staates kann in etwa sechs Monaten erfolgen. In der Ukraine war dies der russische Versuch die Maidan-Bewegung von November 2013 bis Februar 2014 gewaltsam zu brechen. Die daraus resultierende Krise ist meistens bereits mit der Intervention verbunden, wie dem Einmarsch russischer Soldaten auf der Krim im März 2014 oder in der Ostukraine im April 2014. Wenn diese Maßnahmen, aus sowjetischer bzw. heute russischer Sicht nicht ausreich(t)en, um die Verhaltensänderung eines Staates in ihrem Sinne herbeizuführen, erfolgt die Intervention – das Durchführen offensiver Handlungen, bzw. im Fall der Ukraine der Einmarsch im Februar 2022. Erst danach „normalisiert" sich aus sowjetischer Sicht die Situation wieder.[4]

Diese Denkschule gilt noch heute. Wenn Russland bei einem Staat in seiner (selbstdefinierten) Einflusssphäre eine „Ablage" erkennt – sich dieser also nicht so verhält, wie es Moskau möchte –, dann wird nach diesem Schema vorgegangen. Im Falle der Ukraine war es eine zunehmende Annäherung an den Westen, der das Durchlaufen dieser Phasen zur Folge hat. Russland versucht ein Ergebnis zu erzielen, um die erkannte „Ablage" wieder in eine Situation zu bringen, die in seinem Sinne ist. Diese Vorgangsweise ist gut dokumentiert. Zusätzlich gibt es Berichte aus den 1980er- und 1990er-Jahren, unter anderem von ehemaligen KGB-Offizieren, die übergelaufen sind, wie die Schilderungen von Juri Besmenow.[5] Er erklärt in seinen Interviews, dass die durchschnittliche Arbeit eines KGB-Agenten nicht Sabotageaktionen oder die Jagd auf feindliche Agenten ist, wie man vielleicht glauben würde. Die hauptsächliche Agententätigkeit ist vielmehr das Durchführen von subversiven Aktionen und der psychologischen Kriegsführung. Genau das macht Russland zurzeit in unterschiedlichen Ausprägungen in Europa mit einer breiten Palette von hybriden Maßnahmen. Ein Beispiel dafür sind Drohnenüberflüge, die einige westliche Staaten bereits an den Rand einer Krise und die NATO unter Druck gebracht haben.[6]

---

[3] Antoniadis N., Chernyshev A., Höfner R., Lehberger R., Rosenbach M., Schmid F., Schulz T., Weiss M., Wiedmann-Schmidt W., Zeller A., (2026), *Dieser Uni-Lehrstuhl bildet Russlands Cyberkrieger aus, https://www.spiegel.de/ausland/russland-bildet-in-geheimem-uni-programm-spione-und-hacker-fuer-hybriden-krieg-aus-a-2de79023-aa56-4ed6-b5de-d7c222402e63*

[4] Rinaldi, S. (2024), *10 years of Russian annexation of Crimea, reflections on the role of PMCs in hybrid warfare, https://blog.icoca.ch/10-years-of-russian-annexation-of-crimea-reflexions-on-the-role-of-pmcs-in-hybrid-warfare/*

[5] Schett S. (2024), *KGB-Insider packt aus: So funktioniert Destabilisierung, https://materie.at/a/kgb-insider-packt-aus-so-funktioniert-destabilisierung/*

[6] Melchior J. K. (2025), *NATO Has Seen the Future and Is Unprepared – A simulation of drone warfare shows how far the alliance has to go to learn the lessons of Ukraine., https://www.wsj.com/opinion/nato-has-seen-the-future-and-is-unprepared-887eaf0f*

Gezielter Angriff auf die Gesellschaft

Um die Gesellschaft eines Staates zu demoralisieren, kann man versuchen, einen Keil zwischen die Bevölkerung und die Staatsführung zu treiben. Konkret sollen die Bürger das Vertrauen in die Politik verlieren. Aktuell scheint der Angreifer in Europa dafür einen „fruchtbaren Nährboden" vorzufinden. In diesem Zusammenhang stellt sich die Frage, ob die europäischen Staaten bzw. ihre Gesellschaften so resilient sind, dass sie einer hybriden Kriegsführung etwas entgegensetzen können oder ob sie bereits von der Angst getrieben werden. Um diese Frage zu beantworten, hilft ein Blick auf das laufende Tagesgeschehen. Im Jahr 2025 gab es eine Diskussion darüber, ob eingefrorene russische Gelder für die Unterstützung der Ukraine verwendet werden sollen. Dabei spitzte sich die Diskussion rasch zu. Konkret wehrte sich Belgien dagegen, dieses Geld anzugreifen, da es Repressalien von Russland befürchtete. Schließlich wurde davon abgesehen und es gab einen Kompromiss: 90 Milliarden Euro für die Unterstützung der Ukraine sollten aus den Budgets der EU-Staaten kommen. Das führte zum Widerstand anderer EU-Staaten, wie Ungarn, die der Ukraine kein Geld mehr geben wollen. [7]

Mittlerweile gab es bereits Sabotageaktionen, die der beschriebenen Logik folgend, der Intervention zuzurechnen sind. Alleine seit 2022 sind über fünfzig Sabotageangriffe mutmaßlich von Russland in Europa verübt worden. Russland versucht gesamtstaatlich alle Maßnahmen zu bündeln, um quasi anzugreifen. Es gibt zahlreiche Arbeiten, die zeigen, dass die bisherigen Aktionen keine Zufälle oder Einzelfälle waren. Vielmehr handelte es sich dabei um gezielte Angriffe, von denen jeder EU-Staat in Zukunft noch mehr betroffen sein könnte. Das gilt nicht nur für Staaten im Osten, sondern auch für solche im Zentrum Europas, die aufgrund ihrer geografischen Lage nicht mit einem solchen rechnen. [8]

Grüne Männchen, fünf Bären – Ausspähen, Beeinflussen, Sabotieren

Im Jahr 2014 gab es auf der Krim das Phänomen der kleinen grünen Männchen. Das waren russische Soldaten, die ohne Kennzeichnung in die Ukraine marschiert waren. Damals sagte der russische Präsident Vladimir Putin, dass dies Unbekannte wären, die sich in Army Shops russische Uniformen gekauft hätten, aber keine Angehörigen der Streitkräfte der Russischen Föderation. Diese Methode wird immer wieder angewandt. So erschienen im Jahr 2025 offensichtlich russische Soldaten an der estnischen Grenze, was an die Situation der grünen Männchen auf der Krim erinnerte. Mitte März 2026 wurde in russischen sozialen Netzwerken ein „Volksrepublik Narva" propagiert. Es wurde die Autonomie der estnischen Stadt Narva und der gesamten Region Ida-Viru gefordert. Man habe bereits eine gemeinsame Flagge, eine „Hymne" und sogar Pläne für eine „Miliz". In den Beiträgen ist von der „Wahrung der russischen Identität" die Rede. [9]

Bei der Betrachtung des Angreifers betreten die sogenannten „fünf Bären" die Manege. Bei diesen handelt es sich um die fünf wesentlichen Organisationen, die auf russischer Seite gesamtstaatlich versuchen, die vier Phasen Demoralisierung, Destabilisierung, Krise und Intervention umzusetzen. Es sind dies:

- **das russische Außenministerium;**

[7] Sorgi G. (2026), *EU heavyweight Italy joins Belgium in opposing Russian frozen assets plan, https://www.politico.eu/article/eu-italy-joins-belgium-opposing-russia-frozen-assets-plan/*

[8] Olech A., Smolen J., Wojciechowska A. (2026), *Poland as a Target of Russian Hybrid Attacks., https://defence24.com/geopolitics/report-poland-as-a-target-of-russian-hybrid-attacks*

[9] Boffey D. (2025), *'A big chance for the populists': Estonian city alert to the threat of Moscow in its mayoral election, https://www.theguardian.com/world/2025/sep/27/estonia-city-mayoral-election-moscow-threat*

- **der militärische Nachrichtendienst (GRU),**
- **der zivile Geheimdienst (SVR),**
- **der Inlandsgeheimdienst (FSB, der Nachfolger des KGB);**
- **das russische Verteidigungsministerium.**

Die fünf Bären bedienen sich einer Reihe von Wegen und Mitteln, um ihre Ziele zu erreichen. Ihre wesentliche Domäne ist der Cyberraum. Dort sammeln sie Informationen oder führen Beeinflussungsmaßnahmen durch. Bei ihren Operationen gelangen nicht nur potente Staaten ins Visier, sondern auch kleinere, die das vielleicht nicht vermuten oder sich als neutral betrachten. Beim Ausspähen wird die kritische Infrastruktur gezielt identifiziert und in weiterer Folge bereits unterwandert bzw. infiltriert. Das ist die verdeckte Absicht der Zielerreichung und geschieht im Verborgenen. Es gibt zwar immer wieder Berichte über festgenommene Spione, dies werden aber oft als mediale Randnotiz leicht übersehen und sind nur Puzzleteile des gesamten Bildes. [10]

Die Beeinflussung soll eine Verhaltensänderung beim angegriffenen Staat und seiner Regierung bewirken. Ein Beispiel dazu ist die Unterwanderung der Friedensbewegung in den 1970er- und 1980er-Jahren durch sowjetische Agenten. Diese versuchten, die Verteidigungsbereitschaft der Gesellschaften diverser Staaten Europas und vor allem der NATO zu schwächen. Aktuell wird die migrantische Community gezielt von den Russen in verdeckter Art und Weise angesprochen bzw. missbraucht. Ein Beispiel dafür sind abgeschnittene Schweineköpfe, die in Frankreich gezielt vor Moscheen platziert wurden, um die migrantisch-islamische Community aufzuwiegeln. Es konnte eindeutig nachgewiesen werden, dass dafür von Russland Netzwerke der serbischen organisierte Kriminalität in Frankreich angeleitet wurden. Solche Aktionen sollen einen Keil zwischen die Bevölkerungsgruppen treiben, aber auch zwischen diesen und der Regierung. [11]

Um beeinflussen zu können und dazu in der Cyber-Domäne bzw. im Informationsraum wirksam zu werden, bedient sich die Russische Föderation unterschiedlicher Institutionen. Beispiele dazu sind Nachrichtensender oder Social-Media-Kanäle. Diese werden zum Teil von den Geheimdiensten angesteuert und können Russland häufig eindeutig zugeordnet werden. Im Zusammenhang mit solchen Aktionen gäbe es laut dem Generalinspekteur der Deutschen Bundeswehr in Deutschland eine weit verbreitete Realitätsverweigerung. Die Bevölkerung wolle nicht wahrhaben, dass sie das Ziel dieser russischen Angriffe sei, obwohl dies deutlich sichtbar wäre, wenn man hinsehen würde. Es gibt aber auch Elemente, die im Verborgenen als sogenannte „Trolle“ aktiv werden. Das kann man sich wie bei einer russischen Puppe (Matrjoschka) vorstellen. Die wahre Absicht einer Maßnahme bleibt verborgen und zeigt sich erst, wenn alle Schichten durchdrungen sind und man zum Kern vorgedrungen ist. Das entspricht der alten russischen Tradition der Täuschung, der Maskirowka. [12]

Wenn die Beeinflussung nicht ausreicht, um ein Ziel zu erreichen, werden Sabotageaktionen durchgeführt. Seit dem Beginn des Ukraine-Krieges gibt es einige Beispiele, wie auf dem Gebiet von EU-Staaten agiert wird:

- in Schweden gab es Anschläge auf Kommunikationsmasten, die zerstört wurden;

[10] Flade F. (2026), *"Wegwerf-Agenten" auf der A6?, https://www.tagesschau.de/investigativ/wdr/agenten-spionage-ukraine-russland-lettland-100.html*

[11] The Guardian. (2025), *Eleven arrested for placing pigs' heads near French mosques and other hate crimes., https://www.theguardian.com/world/2025/sep/29/eleven-arrested-for-placing-pigs-heads-near-french-mosques-and-other-hate-crimes*

[12] UK-Parliament (2026), *Disinformation diplomacy: How malign actors are seeking to undermine democracy., https://committees.parliament.uk/work/8818/disinformation-diplomacy-how-malign-actors-are-seeking-to-undermine-democracy/*

- in Norwegen versuchten Unbekannte über den Cyberraum in einen Damm einzudringen, um dort die Schleusen zu kontrollieren;

- in Polen, das massiv von Sabotageversuchen betroffen ist, gab es unter anderem einen Anschlagsversuch auf die Wasserversorgung und den Versuch, einen Zug entgleisen zu lassen, indem man Gleise sprengte;

- in internationalen Gewässern wird die kritische Infrastruktur ausgespäht, wie Lines of Communication unter See, also Gas- und Ölpipelines oder Internet-Verbindungskabel,

Diese Beispiele zeigen, dass Russland über ein großes Agentennetz in Europa verfügt, was zahlreiche Enttarnungen bestätigen. Es gibt Untersuchungen unterschiedlicher Think Tanks, die Daten zu den bisherigen Anschlägen sammeln, auswerten und diese auch online publizieren.[13]

Wegwerfagenten, Drohnenflüge – Stellvertreterhandlungen, Verunsicherung

Das führt zu der Frage, wo und wer die Agenten sind, die Anschläge in EU-Staaten durchführen. In den wenigsten Fällen sind es tatsächlich russische Agenten, vielmehr werden sogenannte „Wegwerfagenten" engagiert. Wie sie agieren und warum es so schwierig ist, sie zu ertappen zeigen Beispiele der Deutschen Marine. Dort sind Wegwerfagenten offensichtlich gegen Schiffe vorgegangen, wie drei Beispiele belegen, über die in öffentlichen Medien berichtet wurden:

- Bei einer Korvette gab es den Versuch, Strahlkies in den Antriebsstrang bzw. Motorblock einzubringen. Das gelang zwar, wurde aber bei einer Kontrolle durch Zufall erkannt. Wäre das Schiff ausgelaufen, hätten sich der Strahlkies im Antriebsstrang verkeilt und dort schwere Schäden verursacht.

- Bei einer Fregatte versuchten Unbekannte, Altöl in die Trinkwasseranlage einzuleiten, was ebenfalls nur durch Zufall erkannt wurde. Hätte das funktioniert, wäre eine Komplettreinigung nötig gewesen.

- Bei einem Minenjagdboot haben Unbekannte an mehreren Stellen mit einer Axt versucht, die Kabelbäume zu durchtrennen und das tatsächlich geschafft.

Diese Angriffe sind keine kriegerischen Handlungen, die mit dem Einsatz von Torpedos von einem U-Boot gegen ein Schiff vergleichbar sind. Zusätzlich ist es schwierig zu beweisen, von wem diese Aktionen durchgeführt wurden und ob es tatsächlich von Moskau engagierte Wegwerfagenten waren. In allen drei Fällen wären die Schiffe für Monate ausgefallen und nicht für Einsätze zur Verfügung gestanden. Im Februar 2026 erfolgte die Festnahme von zwei Verdächtigen.[14]

Wegwerfagenten werden aktuell über soziale Medien angeworben. Man wird zum Beispiel auf einem Messenger in eine Gruppe eingeladen. Dort erhält man das Angebot mit kleinen Aktionen Geld zu verdienen. Im Falle der „Schiffssabotageaktionen" könnte dies wie folgt geschehen sein: Ein Wegwerfagent erhält den Auftrag für eine Bezahlung von vielleicht 1 000 Euro Strahlkies in einem Baumarkt zu kaufen und diese an einer Adresse abzugeben. Der nächste Wegwerfagent nimmt diese dort an sich und bringt sie bis zur Werft, wo er sie davor in einen

[13] Connor R. (2026), *Germany summons Russian ambassador over 'hybrid' attacks., https://www.dw.com/en/germany-summons-russian-ambassador-over-hybrid-attacks/a-75129486*
[14] Web.de. (2026), *Sabotageversuch an deutschen Kriegsschiffen., https://www.wsj.com/opinion/nato-has-seen-the-future-and-is-unprepared-887eaf0f*

Mistkübel wirft. Nun kommt der dritte Agent, möglicherweise ein Werftarbeiter, der vielleicht 2 000 Euro erhält und den Strahlkies so platziert, dass er einen gravierenden technischen Schaden verursacht. [15]

Keine einzige dieser Aktionen hat einen unmittelbaren Bezug zur Russischen Föderation oder zu den russischen Geheim- und Nachrichtendiensten. Diese waren jedoch in den sozialen Netzwerken aktiv, wo sie mit Geld Agenten für kleine Aufgaben geködert haben, die dadurch nicht die gesamte Aktion erkennen können. Selbst wenn diese gefasste werden, ist ein Bezug zu Russland schwer nachzuweisen. Die hybriden Angriffe auf die strategische Tiefe Europas sollen vor allem den Nachschub von Versorgungsgütern unterbinden, die für die Ukraine wichtig sind, um diesen Krieg weiterführen. Konkret sollen die europäischen Staaten zu einer Verhaltensänderung bewegt werden und den Nachschub drosseln oder überhaupt einstellen. Europa, vor allem der Zentralraum mit Staaten wie Deutschland, ist aufgrund seiner geografischen Lage eine Drehscheibe, für die Verteilung von Gütern. Dadurch gelangt dieser Raum in das Visier. [16]

In den letzten Monaten gab es immer wieder Versuche, Unruhe mit Drohnenflügen zu stiften. So saßen auf dem Münchener Flughafen aufgrund von Drohnensichtungen plötzlich 6 500 Passagiere fest. Durch solche Aktionen werden viele Personen „getroffen", eine breite Öffentlichkeit betroffen gemacht so und eine große Wirkung erzielt. Drohnenflüge können verschiedene Gründe haben. So kam es in Polen oder Rumänien aufgrund von russischen Luftangriffen auf Ziele in der Ukraine zu Einflügen russischer Drohnen. Zum Teil war das Zufall, teilweise aber Absicht, wie in Polen, wo Drohnen sogar mehrere hundert Kilometer in die Tiefe des Landes vordrangen. Zusätzlich gibt es Drohnenüberflüge in Staaten mit einer Seeanbindung. Man kann davon ausgehen, dass diese Drohnen von Schiffen aus eingesetzt werden, die sich in internationalen Gewässern befinden. [17]

Diese Drohnenüberflüge verfolgen konkrete Ziele. Einerseits werden Routen ausgespäht, auf denen Waffen in die Ukraine geliefert werden. Andererseits sollen Militärbasen für mögliche Folgeaktionen aufgeklärt bzw. die kritische Infrastruktur ausspioniert werden. Oft soll die Präsenz von Drohnen über Objekten „einfach nur" für Angst und Schrecken zu sorgen. Das eigentliche Ziel besteht aber nicht nur darin, die Bevölkerung in Angst und Schrecken zu versetzen. Vielmehr soll diese die Frage stellen, ob die Lufträume ausreichend geschützt wären und warum diese Drohnen nicht vom Himmel geholt werden können. Die Antwort auf solche Fragen kann darin resultieren, dass die europäischen Staaten immer weniger Fliegerabwehrmittel in die Ukraine senden, weil sie diese zu Hause benötigen. Wenn das geschieht, hätte Russland die ukrainische Luftabwehr durch eine hybride Kampagne in Europa geschwächt. Das Ziel, ihre Luftwirkmittel effizienter einzusetzen, würde dann „durch die Hintertüre" erreicht werden. Vorfälle bei denen auch ukrainische Drohnen im Baltikum zu Boden gehen, werden von russischen Medien gezielt genützt um weitere Verunsicherung zu schaffen oder die eigenen Attacken zu verschleiern. [18]

Die Russische Föderation agiert nicht alleine. Sie wird wesentlich von China, Nordkorea oder Indien unterstützt. Diese Staaten verfolgen damit ihre eigenen Ziele. So hat der chinesische Außenminister Wang Yi bei einem Besuch in Europa gegenüber der EU-Außenbeauftragten Kallas

---

[15] Rosenbach M., Schmid F., Sperber S., Yüksel Y. (2025), *Wie Putins Schattenkrieger schon jetzt Deutschland angreifen., https://www.spiegel.de/politik/sabotage-spionage-cyberangriffe-putins-schattenkrieger-in-deutschland-podcast-a-2980b2ad-7445-4b03-a8ae-344df738208a*

[16] Fürsen R. (2026), *Deutschland im Konfliktfall „priorisiertes Ziel" für weitreichende Waffen Russlands., https://www.welt.de/politik/deutschland/article695779eb04e7d12184982970/operationsplan-der-regierung-deutschland-im-konfliktfall-priorisiertes-ziel-fuer-weitreichende-waffen-russlands.html*

[17] Aikmann, I. (2025), *Drones seen over Danish military bases in latest air disruption, https://www.bbc.com/news/articles/c3rvzdq93yro*

[18] Laizans J., Sytas A. (2025), *Baltic nations seek more NATO defence as drone hits Latvian oil tanks, https://www.reuters.com/world/two-drones-russia-crash-latvia-army-says-2026-05-07/*

klargestellt, dass es nicht im Interesse Chinas sei, wenn Russland diesen Krieg verlieren würde. Denn dann könnten sich die USA wieder vermehrt China zuwenden und das möchte man verhindern. Deshalb überrascht es nicht, dass chinesische Schiffe bei hybriden Angriffen eine Rolle spielen. So „verlieren" chinesische Schiffe immer wieder ihre Anker. Diese ziehen sie dann „unbemerkt" über mehrere hundert Kilometer nach, wobei sie „zufällig" kritische Infrastruktur auf dem Meeresboden zerstören. In diesem Zusammenhang ist zu erwähnen, dass China ein Patent für diese Methode angemeldet hat und somit über die Fähigkeit verfügt, solche Maßnahmen durchzuführen. [19]

Auswirkung auf Österreich – Folgen und Chancen

Durch seine geografische Lage im „Herzen Europas" rückt auch Österreich in den Fokus. Österreich hat als Drehscheibe beispielsweise eine zentrale Rolle für die Stromversorgung Europas. Bei überregionalen Herausforderungen, wie Strommangellagen oder gar Blackouts sind die Speicher- und Flusskraftwerke der Alpenrepublik bedeutend. Deshalb sollte Österreich seine kritische Infrastruktur genau beobachten und sichern. Das betrifft nicht nur die Einrichtungen zur Stromversorgung, sondern auch das Öl- und Gasnetz, sowie das Eisenbahn- und Straßennetz. Schließlich wäre es im Falle eines Konfliktes für die NATO essentiell rasch Kräfte von Westen Richtung Osten zu transportieren – durch Österreich. Die Sabotage des Eisenbahn- und Straßennetzes hätte schwerwiegende Folgen auf die militärische Transportlogistik.

Die Herausforderungen der europäischen Staaten durch die zunehmende hybride Kriegsführung kann auch als Chance verstanden werden. Sie könnte ein Weckruf sein, um sich ernsthafte Gedanken über alle Aspekte der Landesverteidigung zu machen, die Rolle der Verbündeten zu evaluieren und daraus resultierend die strategischen Ziele zu überdenken bzw. neu zu formulieren und daraus Konsequenzen abzuleiten, die in konkreten Maßnahmen resultieren, die tatsächlich umgesetzt werden. Es ist bemerkenswert, dass die Bundesrepublik Deutschland bereits überlegt, Sabotage als vorgestaffelte Kriegshandlung einzustufen. Damit wäre ein Fall für die militärische Landesverteidigung gegeben und militärische Mittel würden zum Einsatz kommen, um diesen Angriffen einen Riegel vorzuschieben. Die Europäer sind jedenfalls gefordert, den Ernst der Lage zu erkennen und zu versuchen, gesamtstaatliche und gesamteuropäische Lösungen zu finden, um hybride Angriffe zu erkennen, zu verhindern oder abzuwehren. Jedem muss bewusst sein: Diese Gefahr ist keine Verschwörungstheorie, sie ist real und aktuell – nicht irgendwann oder irgendwo, sondern hier und jetzt. [20]

[19] Jamston.org (2025), *Creative Destruction: PRC Undersea Cable Technology, https://jamestown.org/creative-destruction-prc-undersea-cable-technology/*

[20] Bajarunas, E. (2025), *The Hybrid Threat Imperative: Deterring Russia before it is too late, https://cepa.org/comprehensive-reports/the-hybrid-threat-imperative-deterring-russia-before-it-is-too-late/*

Dr. Markus Reisner, PhD Oberst des Generalstabsdienstes

Geb. 1978; Offizier des österreichischen Bundesheeres, Dr.-Studium der Geschichte sowie PhD-Studium der Rechtswissenschaften an der Universität Wien; wiederholte Auslandsverwendungen und -einsätze in Bosnien und Herzegowina, Kosovo, Afghanistan, Irak, Tschad, Zentralafrika und Mali; Verwendung im Bundesministerium für Europäische und Internationale Angelegenheiten; Forschungsschwerpunkte: Einsatz und Zukunft von unbemannten Aufklärungs- und Waffensystemen, historische und aktuelle militärische Themenstellungen; Verfasser mehrerer Bücher; seit März 2024 Leiter des Institut für Offiziersausbildung an der Theresianischen Militärakademie und somit verantwortlich für die Grundausbildung aller österreichischen Offiziere.

Quellenverzeichnis:

Aikmann, I. (2025), *Drones seen over Danish military bases in latest air disruption, https://www.bbc.com/news/articles/c3rvzdq93yro*

Antoniadis N., Chernyshev A., Höfner R., Lehberger R., Rosenbach M., Schmid F., Schulz T., Weiss M., Wiedmann-Schmidt W., Zeller A., (2026), *Dieser Uni-Lehrstuhl bildet Russlands Cyberkrieger aus, https://www.spiegel.de/ausland/russland-bildet-in-geheimem-uni-programm-spione-und-hacker-fuer-hybriden-krieg-aus-a-2de79023-aa56-4ed6-b5de-d7c222402e63*

Bajarúnas, E. (2025), *The Hybrid Threat Imperative: Deterring Russia before it is too late, https://cepa.org/comprehensive-reports/the-hybrid-threat-imperative-deterring-russia-before-it-is-too-late/*

Biermann, K. (2026), *So führen russische Söldner ihren Schattenkrieg gegen Europa, https://www.zeit.de/politik/ausland/2026-02/geheimdienst-gru-russland-soeldner-sabotage-wagner-gruppe*

Boffey D. (2025), *'A big chance for the populists': Estonian city alert to the threat of Moscow in its mayoral election, https://www.theguardian.com/world/2025/sep/27/estonia-city-mayoral-election-moscow-threat*

Connor R. (2026), *Germany summons Russian ambassador over 'hybrid' attacks., https://www.dw.com/en/germany-summons-russian-ambassador-over-hybrid-attacks/a-75129486*

Flade F. (2026), *"Wegwerf-Agenten" auf der A6?, https://www.tagesschau.de/investigativ/wdr/agenten-spionage-ukraine-russland-lettland-100.html*

Fürsen R. (2026), *Deutschland im Konfliktfall „priorisiertes Ziel" für weitreichende Waffen Russlands., https://www.welt.de/politik/deutschland/article695779eb04e7d12184982970/operationsplan-der-regierung-deutschland-im-konfliktfall-priorisiertes-ziel-fuer-weitreichende-waffen-russlands.html*

Jamston.org (2025), *Creative Destruction: PRC Undersea Cable Technology, https://jamestown.org/creative-destruction-prc-undersea-cable-technology/*

Melchior J. K. (2025), *NATO Has Seen the Future and Is Unprepared – A simulation of drone warfare shows how far the alliance has to go to learn the lessons of Ukraine., https://www.wsj.com/opinion/nato-has-seen-the-future-and-is-unprepared-887eaf0f*

Rinaldi, S. (2024), *10 years of Russian annexation of Crimea, reflections on the role of PMCs in hybrid warfare, https://blog.icoca.ch/10-years-of-russian-annexation-of-crimea-reflexions-on-the-role-of-pmcs-in-hybrid-warfare/*

Olech A., Smolen J., Wojciechowska A. (2026), *Poland as a Target of Russian Hybrid Attacks., https://defence24.com/geopolitics/report-poland-as-a-target-of-russian-hybrid-attacks*

Rosenbach M., Schmid F., Sperber S., Yüksel Y. (2025), *Wie Putins Schattenkrieger schon jetzt Deutschland angreifen., https://www.spiegel.de/politik/sabotage-spionage-cyberangriffe-putins-schattenkrieger-in-deutschland-podcast-a-2980b2ad-7445-4b03-a8ae-344df738208a*

Schett S. (2024), *KGB-Insider packt aus: So funktioniert Destabilisierung, https://materie.at/a/kgb-insider-packt-aus-so-funktioniert-destabilisierung/*

Sorgi G. (2026), *EU heavyweight Italy joins Belgium in opposing Russian frozen assets plan, https://www.politico.eu/article/eu-italy-joins-belgium-opposing-russia-frozen-assets-plan/*

The Guardian. (2025), *Eleven arrested for placing pigs' heads near French mosques and other hate crimes., https://www.theguardian.com/world/2025/sep/29/eleven-arrested-for-placing-pigs-heads-near-french-mosques-and-other-hate-crimes*

UK-Parliament (2026), *Disinformation diplomacy: How malign actors are seeking to undermine democracy., https://committees.parliament.uk/work/8818/disinformation-diplomacy-how-malign-actors-are-seeking-to-undermine-democracy/*

Web.de. (2026), *Sabotageversuch an deutschen Kriegsschiffen., https://www.wsj.com/opinion/nato-has-seen-the-future-and-is-unprepared-887eaf0f*