

März

Oliver Drewes*

Russische Spionage und Sabotage in Deutschland – Hybride Kriegsführung ohne Kriegserklärung

Das parlamentarische Kontrollgremium (PKGr) des Bundestages ist eine zentrale Kontrollinstanz zur Überwachung der drei deutschen Nachrichtendienste: des Militärischen Abschirmdienstes (MAD), des Bundesnachrichtendienstes (BND) und des Bundesamtes für Verfassungsschutz (BfV). Für gewöhnlich äußert sich das PKGr selten öffentlich zur Arbeit der Nachrichtendienste und zu sicher-

heitspolitischen Entwicklungen; Umso genauer sollte man hinhören, wenn es eine irreguläre Unterrichtung herausgibt und damit eine Warnung ausspricht.

Mitte März 2024 veröffentlichte das PKGr eine Lageeinschätzung über die zunehmenden und besorgniserregenden Spionage- und Sabotagefälle durch Russland in Deutschland.¹ Der Tenor des



Die drei aktuellen Präsidenten der deutschen Nachrichtendienste: Thomas Haldenwang (BfV), Martina Rosenberg (MAD) und Bruno Kahl (BND) bei der öffentlichen Anhörung im Parlamentarischen Kontrollgremium 2023²

* DOI: <https://doi.org/10.25353/ubtr-2d35-b08c-b067>

¹ Parlamentarisches Kontrollgremium (2024): PKGr-Bewertung der „russischen Einflussnahme in Deutschland“. URL: <https://www.bundestag.de/presse/hib/kurzmeldungen-993564> [29.11.2024].

² Redaktionell eingefügtes Bild: Copyright: Deutscher Bundestag, Sebastian Rau, photothek.

Papiers: Der außenpolitische Umgang miteinander wird rauer und vor allem handfest. Auch wenn Deutschland darauf bedacht ist, nicht aktiv in den militärischen Konflikt zwischen Russland und der Ukraine hineingezogen zu werden, also in keinen Kriegszustand zu geraten, kann von friedlichen Verhältnissen immer weniger die Rede sein. Im Folgenden wird der Versuch unternommen, einen Überblick über die zahlreichen russischen Aktivitäten in Deutschland (und Europa), auf die das PKGR nur cursorisch verweist, zu geben.

Einflussnahme

Im Kontext des Angriffskrieges Russlands auf die Ukraine finden intensive Debatten darüber statt, wie die Konfliktsituation zu bewerten ist und inwieweit man Unterstützung leisten sollte. Den Verlauf dieses Diskurses will Russland aus strategischen Gründen in seinem Sinne beeinflussen.³ Sichtbar wurden dabei in den sozialen Netzwerken neue Medienportale, die eine Berichterstattung in auffallend prorussischer Haltung verbreiten.⁴ Dass es Medien wie Russia-Today, Sputnik oder Voice of Europe gibt, die russische Propaganda verbreiten, ist soweit nicht verwunderlich und nichts Neues. Auch Täuschungsaktionen, bei denen Nachrichtenwebseiten breit rezipierter deutscher Medien wie *Spiegel*, *WELT* und *BILD* täuschend echt nachgebaut wurden, sind nicht

erst 2024 aufgekommen. Desinformationskampagnen, wie die solcher „Doppelgänger“, nehmen aber an Umfang, Organisiertheit und Aktivität zu.⁵ Das Auswärtige Amt bezifferte z.B. speziell die Aktivität der Doppelgänger-Kampagne, die vom russischen Unternehmen *Social-Design-Agency (SDA)* durchgeführt wurde, mit einer Posting-Rate von zwei Millionen Posts auf X (ehem. Twitter) innerhalb eines Tages.⁶ Während der ersten vier Monate im Jahr 2024 hat die *SDA* knapp 34 Millionen Kommentare gepostet, etwa 40.000 mediale Inhalte (v.a. Bilder) verbreitet sowie 4600 Videos produziert.⁷ Dass es Unternehmen gibt, die Trollfarmen⁸ anlegen und die sozialen Medien mit Bots fluten, ist in Russland kein Geheimnis (mehr)⁹: Bekannt war z.B. die *Internet Research Agency*, die von dem ehemaligen Wagner-Kommandeur Yevgeny Prigozhin gegründet wurde (heute aber nicht mehr aktiv ist).¹⁰ Inzwischen intensivieren sich auch die Verbindungen zwischen den Akteuren von Desinformationskampagnen und cyberkriminellen (Maleware-)Attacken auf Unternehmen und politische Institutionen – politische Propagandaaktivität und gewinnorientierte Kriminalität verschmilzt.¹¹ Der Umfang der Desinformationskampagnen und der Aufwand, der betrieben wird, sind immens und weiten sich aggressiv aus.¹² Die *SDA*, die nur als öffentlich bekannt gewordenes Beispiel gelten kann, formiert sich bewusst als Werkzeug

- 3 Bundesministerium des Innern und für Heimat. (2024): *Desinformation im Zusammenhang mit Russlands Angriffskrieg auf die Ukraine*. URL: <https://www.bmi.bund.de/SharedDocs/schwerpunkte/DE/desinformation/desinformation-russlands-angriffskrieg.html> [29.11.2024].
- 4 Spiegel (2022): Gefälschte Nachrichtenseiten verbreiten prorussische Propaganda. URL: <https://www.spiegel.de/netzwelt/web/fake-news-von-sockenpuppen-gefaelschte-deutsche-nachrichtenwebsites-kursieren-auf-facebook-a-6a4308b3-b15f-4606-8f65-a78a74857e33> [29.11.2024].
- 5 EU Desinfo Lab (2024): That is the Doppelgänger Operation?. URL: <https://www.disinfo.eu/doppelgaenger-operation/> [29.11.2024]; Qurium (2024): How Russia uses EU Companies for Propaganda. URL: <https://www.qurium.org/alerts/exposing-the-evil-empire-of-doppelgaenger-disinformation/> [29.11.2024]; U.S. Cybercommand (2024): Russian Disinformation Campaign Doppelgänger unmasked. A Web of Deception. URL: <https://www.cybercom.mil/Media/News/Article/3895345/russian-disinformation-campaign-doppelgaenger-unmasked-a-web-of-deception/> [29.11.2024].
- 6 Süddeutsche Zeitung (2024): Im Auftrag des Kreml wird russische Desinformation in den sozialen Medien verbreitet. URL: <https://www.sueddeutsche.de/projekte/artikel/politik/russland-propaganda-desinformation-social-design-agency-ilja-gambaschidse-sofia-sacharowa-facebook-telegram-memes-karikaturen-putin-ukraine-krieg-in-der-ukraine-e843184?reduced=true> [29.11.2024].
- 7 Der Standard (2024): Datenleck belegt millionenfache Einflussnahme russischer Internettrolle. URL: <https://www.derstandard.de/story/3000000237148/datenleck-belegt-millionenfache-einflussnahme-russischer-internettrolle> [29.11.2024].
- 8 Eine Trollfarm ist eine organisierte Gruppe, die gezielt Desinformation, Propaganda oder manipulative Inhalte im Internet verbreitet. Sie besteht meist aus mehreren Personen, die unter einer sehr großen Zahl falscher Identitäten („Trolle“) auf sozialen Medien, Foren oder Kommentarspalten agieren, um Meinungen zu beeinflussen, Debatten zu stören oder gesellschaftliche Spaltungen zu vertiefen.
- 9 Besonders ausführlich zu den russischen Trollfarmen: Aro, J. (2022): *Putins Armee der Trolle – Der Informationskrieg des Kreml gegen die demokratische Welt*. Goldmann Verlag.
- 10 Spyscape (2024): Inside Russia's Notorious 'Internet Research Agency' Troll Farm. URL: <https://spyscape.com/article/inside-the-troll-factory-russias-internet-research-agency> [29.11.2024]; University of Melbourne (2021): Understanding Mass Influence. A case study of the Internet Research Agency as a contemporary mass influence operation. URL: <https://www.unsw.edu.au/content/dam/pdfs/unsw-adobe-websites/canberra/research/defence-research-institute/2023-02-Understanding-Mass-Influence---A-case-study-of-the-Internet-Research-Agency.pdf> [29.11.2024].
- 11 EU Desinfo Lab (2024): Yet more evidence of Russia's boundless impunity to spread misinformation in the EU. URL: <https://www.disinfo.eu/publications/yet-more-evidence-of-russias-boundless-impunity-to-spread-misinformation-in-the-eu/> [29.11.2024].
- 12 CeMAS (2024): Fortsetzung folgt: Die prorussische Desinformationskampagne Doppelgänger in Deutschland. URL: <https://cemas.io/publikationen/fortsetzung-folgt-doppelgaenger/> [29.11.2024].

digitaler Kriegsführung. In Materialien der *SDA*, die die *Süddeutsche Zeitung* zitiert, wird ihr Selbstverständnis deutlich: „Das Schlachtfeld sind die Köpfe der Bewohner des Planeten Erde. Dieses Schlachtfeld gehört uns.“¹³

Wahlbeeinflussung und finanzielle Unterstützung

In den letzten Jahren standen immer wieder Vorwürfe im Raum, Russland habe versucht, Einfluss auf Wahlkämpfe zu nehmen. Das geschieht durch die oben beschriebenen Propaganda- und Desinformationskampagnen, aber auch durch die Unterstützung von Politikern und Parteien, die Russland politisch zugeneigt sind. Zwar ist eine eindeutige Beeinflussung von Wahlen und Politikern schwer zu belegen, aber die Masse an belastenden Hinweisen wiegt schwer¹⁴ – im Fall der Beeinflussung der US-Wahlen 2016 sind sich die US-Geheimdienste sicher, dass es eine von Putin angewiesene Kampagne gab.¹⁵ Zwar manipulieren russische Akteure nicht den Wahlprozess an sich, doch aber den Wahlkampf: Das niederländische Forschungsnetzwerk *Trollensics* hat z.B. in den großen Desinformationskampagnen aus Russland eine systematische Unterstützung der AfD gefunden.¹⁶ Das Ziel: Die Zukunftsangst der Bevölkerung schüren und so (russlandfreundlichen) Rechtsaußenparteien zu Wahlgewinnen verhelfen. Das *Organized Crime and Corruption Reporting Project (OCCRP)* berichtet über die Wahl hinausgehend sogar von konkret vorbereiteten Beschlussvorlagen für parla-

mentarische Prozesse in Europa, die im Sinne Russlands sind und die entsprechend sympathisierenden Parteien mitgegeben werden können.¹⁷ Nicht nur inhaltlich, sondern auch in direkt personellem Kontakt wird der Zugang zur Politik gesucht: In Deutschland steht die Einflussnahme auf AfD-Politiker im Raum. Die Generalstaatsanwaltschaft ermittelt 2024 z.B. wegen des Anfangsverdachts auf Bestechlichkeit.¹⁸ Auch in den Jahren zuvor gab es immer wieder Fälle von finanziellen Zuwendungen gegenüber deutschen und europäischen Rechtsaußenpolitikern, die sich an der Grenze der Legalität bewegten.¹⁹ Selbst wenn es keine Rechtsverletzung gab, ist der Versuch, von außen politisch opportune Parteien zu unterstützen, höchst bedenklich.

Mordanschläge

Dass sich Russland mit politischen Operationen gegen politische Gegner im Ausland nicht zurückhält, machen die bemerkenswert offen durchgeführten Mordanschläge deutlich: Alexander Litwinenko wurde 2006 in London mit radioaktivem Polonium-210 vergiftet, Dmitri Kovtun und Andrei Lugowoi auf gleiche Weise zeitnah in Hamburg; Sergei und Julia Skripal 2018 in Salisbury mit dem Nervengift Nowitschok ebenso wie Alexander Nawalny 2020; Zelimkhan Khangoshvili wurde 2019 im Berliner Tiergarten erschossen – die Liste ließe sich erweitern.²⁰ Unlängst teilten US-amerikanische Geheimdienste mit, dass Russland einen Mordanschlag auf den deutschen Vorstandsvorsitzenden des Rüstungskonzerns Rheinmetall Armin Paper-

13 Vgl. Fn. 5.

14 German Marshall Fund (2024): The Many Faces of Foreign Interference in European Elections. URL: <https://www.gmfus.org/news/many-faces-foreign-interference-european-elections> [29.11.2024].

15 National Intelligence Council (2017): Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution. URL: https://www.dni.gov/files/documents/ICA_2017_01.pdf [29.11.2024].

16 Euronews (2024): Russia's second front: How Europe can prepare against hybrid warfare. URL: <https://www.euronews.com/2024/08/24/russias-second-front-how-europe-can-prepare-against-hybrid-warfare> [29.11.2024]; Spiegel (2024): Trollarmeen unterstützten AfD – und Wagenknecht. URL: <https://www.spiegel.de/panorama/propaganda-russische-trollarmeen-unterstuetzen-afd-und-sahra-wagenknecht-in-social-media-a-a73b2343-9013-4d17-81be-a8004c866cb0> [29.11.2024].

17 Organized Crime and Corruption Reporting Project (2023): Kremlin-Linked Group Arranged Payments to European Politicians to Support Russia's Annexation of Crimea. URL: <https://www.occrp.org/en/investigation/kremlin-linked-group-arranged-payments-to-european-politicians-to-support-russias-annexation-of-crimea> [29.11.2024].

18 Flade, F. (2024): Sabotage der Demokratie. URL: <https://ojihad.wordpress.com/2024/05/21/sabotage-der-demokratie/> [29.11.2024].

19 Deutsche Welle (2018): Report: Russian money fueled AfD trip. URL: <https://www.dw.com/en/report-afd-members-flight-sponsored-with-russian-money/a-43872774> [29.11.2024]; Open Democracy (2022): We know Russia funds Europe's far Right. But what does it get in return?. URL: <https://www.opendemocracy.net/en/5050/russia-ukraine-war-putin-europe-far-right-funding-conservatives/> [29.11.2024].

20 Bloomberg (2024): Putin's Assassination Targets Revealed in Declassified Memo. URL: <https://www.bloomberg.com/news/newsletters/2024-11-22/putin-s-assassination-targets-revealed-in-declassified-memo> [29.11.2024].

ger geplant haben soll.²¹ Auch wenn die gezielten (geplanten) Tötungen einzelner Menschen bisher keine internationalen militärischen Konfrontationen zur Folge gehabt haben, lässt sich dennoch die Frage stellen, ab wann Auftragsmorde in Europa einen politisch neuralgischen Punkt erreichen, so dass daraus mehr als nur eine diplomatische Krise folgt.

Spionage

Das gemeinhin als zweitältestes Gewerbe der Welt bezeichnete Feld der Spionage findet mit den stattfindenden Operationen naturgemäß eher selten öffentliche Aufmerksamkeit. Umso wichtiger sind auch hier die Warnungen der Sicherheitsbehörden vor erhöhter ausländischer Spionageaktivität in Deutschland und Europa. Das BfV weist nicht nur regelmäßig in seinen Jahresberichten, sondern zunehmend mehr auch in Sonderberichten und in Beratungsfunktion darauf hin, dass sich die Aktivität v.a. durch Russland und China stark erhöht hat. Die Konzentration der Spionageaktivitäten liegt auf der deutschen Sicherheitsinfrastruktur, sensibler Wirtschaftsstandorte sowie Logistik-, Energie- und Verkehrsstrukturen. Der genaue Umfang lässt sich in Zahlen schwer erfassen; Nur punktuell werden Fälle sichtbar (bzw. von den deutschen Sicherheitsbehörden öffentlich mitgeteilt):

- Ein Mitarbeiter des BND wurde 2023 als Spion für Russland enttarnt;²²

- Immer wieder wird bemerkt, dass Gelände und Ausrüstungsstrukturen der Bundeswehr ausgespäht werden²³ – allein 2023 wurden 446 Drohnensichtungen gemeldet;²⁴
- In der Ostsee sind zunehmend russische Forschungsschiffe aufgefallen, die systematisch hydrographische Aufklärung durchführen und die Lage von Unterseekabeln, Windparks, Pipelines und militärische Infrastruktur auskundschaften;²⁵
- Peinlich wurde das von der russischen Propagandaplattform Russia-Today veröffentlichte abgehörte Gespräch hochrangiger Bundeswehroffiziere, die über deutsche Waffensysteme berieten;²⁶
- Speziell von den russischen Konsulaten und Botschaften in Deutschland ausgehend agierten zahlreiche Diplomaten, Botschaftsangehörige und Geheimdienstler zur Informationsbeschaffung.²⁷

Hacks und Cyberangriffe

Auf den Bundestag, die SPD-Parteizentrale, Luftfahrt- und IT-Unternehmen, Rüstungskonzerne und viele weitere mehr finden nahezu ständig Cyberangriffe statt. Mittels digitaler Forensik sind diese Aktionen sehr häufig auf russische (aber auch chinesische) Akteure zurückzuführen.²⁸ Das Bundesamt für Sicherheit in der Informationstechnik (BSI) machte 2024 22 Advanced Persistent Threats (APT)²⁹ aus, die Behörden und Unternehmen z.B.

21 CNN (2024): Exclusive: US and Germany foiled Russian plot to assassinate CEO of arms manufacturer sending weapons to Ukraine. URL: <https://edition.cnn.com/2024/07/11/politics/us-germany-foiled-russian-assassination-plot/index.html> [29.11.2024].

22 ZDF (2023): Spionageverdacht: BND-Mitarbeiter vor Gericht. URL: https://www.zdf.de/nachrichten/politik/deutschland/prozess-bnd-mitarbeiter-spionage-russland-100.html?utm_source=chatgpt.com [29.11.2024].

23 MAD (2024): MAD-Report. Bericht des Militärischen Abschirmdienstes für das Jahr 2023. URL: <https://www.bundeswehr.de/resource/blob/5836062/ffd7aadddfeda7cd6e960c4ca50e249a/mad-report-2023-data.pdf> [29.11.2024].

24 Tagesschau (2024): Fast 450 Drohnen über Bundeswehrstandorten gesichtet. URL: <https://www.tagesschau.de/investigativ/ndr-wdr/zunahme-drohnensichtungen-100.html> [29.11.2024].

25 Schaller, C. (2024): Russia's Mapping of Critical Infrastructure in the North and Baltic Seas – International Law as an Impediment to Countering the Threat of Strategic Sabotage?. *Nordic Journal of International Law*, 93(2), 202-236. URL: https://brill.com/view/journals/nord/93/2/article-p202_002.xml; <https://ojihad.wordpress.com/tag/marine/> [29.11.2024]; Hybrid CoE (2023): Handbook on maritime hybrid threats: 15 scenarios and legal scans. URL: https://www.hybridcoe.fi/wp-content/uploads/2023/03/NEW_web_Hybrid_CoE_Paper-16_rgb.pdf [29.11.2024].

26 Deutschlandfunk (2024): Worum es bei der Taurus-Abhöraffaire geht. URL: <https://www.deutschlandfunk.de/taurus-leak-bundeswehr-100.html> [29.11.2024].

27 BfV (2024): Verfassungsschutzbericht 2023. URL: https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/verfassungsschutzberichte/2024-06-18-verfassungsschutzbericht-2023.pdf?__blob=publicationFile&v=17 [29.11.2024].

28 Bundesministerium des Inneren und für Heimat (2024): Cyberangriffe stammen von russischem Militärgeheimdienst. URL: <https://www.bmi.bund.de/SharedDocs/kurzmeldungen/DE/2024/05/schutzmassnahmen-cyberangriffe.html> [29.11.2024].

29 Advanced Persistent Threats (APTs) sind gezielte, hochentwickelte Cyberangriffe, die von hochqualifizierten und gut organisierten Akteuren, wie Staaten, staatlich unterstützten Gruppen oder organisierten Kriminellen, durchgeführt werden. Sie haben das Ziel, über einen längeren Zeitraum unbemerkt in ein Netzwerk einzudringen und sensible Daten oder Informationen zu stehlen, Systeme zu sabotieren oder Spionage zu betreiben.

in Cloud-Infrastrukturen, durch Ransomware, Phishing-Kampagnen oder Zero-Day-Schwachstellen angegriffen.³⁰ Das BSI beziffert die Zahl täglich durchschnittlich bekannt werdender Schadprogramme zwischen 2023 und 2024 mit 309.000 Varianten.³¹ Die Schäden, die durch solche Angriffe entstehen, sind dabei immens. Zwar lässt sich nur schwer die Höhe des monetären Schadens durch die speziell russischen Angriffe feststellen, jedoch macht die Höhe von insgesamt etwa 205,9 Mrd. Euro Schaden durch sämtliche Cyberkriminalität im Jahr 2023³² deutlich, dass sich im digitalen Raum empfindliche Schwachstellen der deutschen Gesellschaft und Wirtschaft ergeben.³³

Sabotageakte

In Deutschland ist zwar besonders die Zerstörung der Nord-Stream-2 Pipeline – bei der die Verantwortlichen noch nicht abschließend ermittelt sind – als politisch und wirtschaftlich folgenschwerer Sabotageakt in die öffentliche Aufmerksamkeit gerückt, aber auch darüber hinaus kam es vermehrt zu kleinen Angriffen, die in der Summe erheblichen Schaden anrichteten:

- In Form von Brandstiftung wurde im Mai ein Gebäude des Rüstungskonzerns Diehl Metall stark beschädigt;³⁴
- Sich vorbereitende Saboteure konnten gestoppt werden, die US-Stützpunkte ausspähten und Anschläge auf militärische Transportwege planten;³⁵
- Bisher nicht eindeutig einem Täter zugeordnet,

aber dennoch bemerkenswert ist der Fall von in Paketen versendeten Brandsätzen, die sich entzündeten, sobald sie in logistisch empfindlichen Frachtzentren lagen.³⁶

- Eine besonders kreative Strategie ist der Einsatz von „low level-“ oder „single-use-Agenten“.³⁷ Dabei werden Amateure (häufig anonym via Social Media) gewonnen, die ohne jegliche nachrichtendienstliche Ausbildung oder Anstellung für eine Geldsumme Spionage- und Sabotageakte durchführen. Für Sicherheitsbehörden ist der Rückgriff auf solche „Agenten“ eine sehr große Herausforderung, denn sie können mangels vorausgegangener ideologischer Radikalisierung und Aktivität nur schwer und erst spät entdeckt werden. Sie sind in kein Netzwerk eingebunden und führen daher auch in weiteren Ermittlungen kaum weiter.

Instrumentalisierung und Förderung von Migrationsströmen

Sabotage kann in einem weiteren Sinne auch als bewusste Überforderung eines Systems bis hin zu seinem Zusammenbruch verstanden werden. Was so abstrakt klingt, konkretisiert sich in der Strategie Russlands darin, gezielt Ströme von Einwanderern an die europäischen Außengrenzen (meistens nach Polen, dem Baltikum und Finnland) zu bringen und so die Grenzsicherung und Immigrationskontrolle unter Druck zu bringen.³⁸ Diese Strategie ist von Russland bewusst gewählt, da die Bewältigung und Organisation von Immigration ein Triggerpunkt der europäischen Gesellschaft ist. Gerade gegen

30 BSI (2024): Die Lage der IT-Sicherheit in Deutschland 2024. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2024.pdf?__blob=publicationFile&t=5 [29.11.2024]; vgl. auch Fn. 32.

31 BSI (2024): Cybersicherheit: Bedrohungslage bleibt angespannt, aber Resilienz gegen Angriffe steigt. URL: https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2024/241112_Lagebericht_2024.html [29.11.2024].

32 BKA 2024 – Bundeslagebild Cybercrime 2023. URL: <https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2023.html?nn=28110> [29.11.2024].

33 Bitkom (2024): Angriffe auf die deutsche Wirtschaft nehmen zu. URL: <https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2024#> [29.11.2024].

34 Frankfurter Rundschau (2024): Nach Brand bei deutschem Rüstungskonzern führt die Spur zu Putin – Beweise zerstört. URL: <https://www.fr.de/politik/ukraine-waffen-feuerteufel-putin-russland-brand-deutscher-ruestungskonzern-sabotage-berlin-93147628.html> [29.11.2024].

35 Spiegel (2024): Mutmaßliche russische Saboteure in Bayern verhaftet. URL: <https://www.spiegel.de/politik/deutschland/generalbundesanwalt-ermittelt-zwei-mutmassliche-russische-saboteure-in-bayern-verhaftet-a-0115bebd-195a-41fb-83be-da8d642045cd> [29.11.2024].

36 Tagesschau (2024): Behörden warnen vor Brandsätzen in Paketen. URL: <https://www.tagesschau.de/inland/warnung-brandsaetze-pakete-100.html> [29.11.2024].

37 Die Zeit (2024): Die Wegwerf-Agenten. URL: <https://www.zeit.de/2024/41/russische-sabotage-wegwerf-agenten-geheimdienst-sicherheitsbehoerde> [29.11.2024]; Flade, F. (2024): <https://ojihad.wordpress.com/tag/single-use-agent/> [29.11.2024].

38 The Guardian (2023): Estonia accuses Russia of weaponising immigration at Europe's borders. URL: <https://www.theguardian.com/world/2023/nov/23/estonia-accuses-russia-weaponising-immigration-europe-borders> [29.11.2024]; Mixed Migration Centre (2024): Russo-Finish border games – more serious than they look. URL: <https://mixedmigration.org/russo-finish-border-games/> [29.11.2024].

liberale Demokratien, für die die Anwendung der Menschenrechte und das individuelle Recht auf Asyl ein Selbstanspruch ist, kann Migration instrumentalisiert und als Waffe verwendet werden, um politische Polarisierung anzuheizen.³⁹ Zwar sind die Zahlen im Vergleich mit den Migrationsströmen aus der Ukraine oder dem Nahen Osten gering – knapp 6.000 Einreisen verzeichnete die Bundespolizei 2023 über die Belarus-Route über Polen nach Deutschland⁴⁰ –, aber dennoch stellt die Außen Grenzsicherung eine wachsende Herausforderung für die EU und die betreffenden Länder (und damit später auch Deutschland) dar.

Hybride Kriegsführung

Miteinander im Konflikt stehende Staaten warten nicht immer erst auf eine direkte Kriegserklärung, bis sie beginnen, ihren Gegner zu schwächen oder zu bekämpfen. Dazu werden Mittel gewählt, die unterhalb der Schwelle einer offenen kriegerischen Handlung ansetzen. Die oben angerissenen Handlungswege sind Teil einer modernen hybriden

Kriegsführungsstrategie. Hierbei werden militärische, nicht-militärische und asymmetrische – d.h. nicht gleichermaßen genutzte – Methoden gewählt.⁴¹ Vor dem Hintergrund einer unklaren Konfliktsituation gegenüber Russland beschrieb Generalleutnant der Bundeswehr André Bodemann die Lage als eine diffuse Anspannung: „Wir sind zwar nicht im Krieg, aber wir sind auch schon lange nicht mehr im Frieden. Wir sind in einer Phase dazwischen“⁴² Das Ziel all dieser Aktivitäten: Destabilisierung, Verunsicherung und gesellschaftliche Spaltung. Mit den Mitteln der Spionage und Sabotage kann ein Staat seinem Gegner bereits erheblichen Schaden zufügen und ihn schwächen, ohne ihm den Krieg zu erklären – und das zu, mit einem konventionellen Krieg verglichen, sehr geringen Kosten. Das PKGr im Bundestag kommt vor dem Hintergrund der russischen Vorgehensweisen in seiner an die Öffentlichkeit gerichteten Warnung zum Fazit: „Das Gremium ist überzeugt, dass sich Deutschland zukünftig deutlich robuster, resilienter und wehrhafter aufstellen muss.“⁴³

39 Greenhill, K. (2016): Massenmigration als Waffe – Vertreibung, Erpressung und Außenpolitik. Kopp Verlag, Rottenburg.

40 Merkur (2024): Belarus-Route: 2215 Migranten kamen bis nach Deutschland. URL: <https://www.merkur.de/deutschland/mecklenburg-vorpommern/2215-migranten-kamen-bis-nach-deutschland-belarus-route-zr-93132417.html> [29.11.2024].

41 Bundesministerium des Inneren und für Heimat (2024): Hybride Bedrohungen und Desinformation. URL: <https://www.bmi.bund.de/DE/themen/heimat-integration/wehrhafte-demokratie/abwehr-hybrider-bedrohungen/abwehr-hybrider-bedrohungen-node.html> [29.11.2024].

42 Bundeswehr (2023): „Es geht um den Schutz und die Sicherheit Deutschlands“. URL: <https://www.bundeswehr.de/de/aktuelles/meldungen/nachgefragt-schutz-sicherheit-deutschlands-5694358> [29.11.2024].

43 Vgl. Fn. 1