AUSTRIAN INSTITUTE FOR EUROPEAN AND SECURITY POLICY

Bundesministerium Landesverteidigung

Nr. 2023/3

Die russische hybride Kriegsführung

Im Kontext des Angriffskriegs gegen die Ukraine

von Michael Zinkanell

März 2023

AIES STUDY

Executive Summary

Die russische hybride Kriegsführung gegen die Ukraine hat ihren Ursprung nicht in der militärischen Invasion der Ukraine seit Februar 2022, sondern ist in Ansätzen bereits seit den 2000er Jahren erkennbar und wurde seit der Annexion der Krim 2014 stetig intensiviert. Diese AIES Studie fokussiert sich auf die Analyse der russischen hybriden Kriegsführung seit Februar 2022 und zeigt auf wie der Kreml durch den systematischen Einsatz von hybriden Instrumenten strategisch-militärische Ziele verfolgt.

Dadurch wird die Verschmelzung und Synchronisation von unkonventionell hybriden Taktiken mit der konventionell militärischen Kriegsführung sichtbar. Der Schwerpunkt der Analyse liegt auf der Beurteilung von russischen Cyberangriffen und Desinformationskampagnen, die im Kontext der hybriden Kriegsführung gegen die Ukraine primär zur Anwendung kommen. Darüber hinaus wird einleitend der breitere Kontext der russischen hybriden Kriegsführung dargelegt. Für die österreichische und europäische Sicherheitspolitik ergeben sich aus der Intensivierung der russischen hybriden Kriegsführung ernstzunehmende Herausforderungen, denn die russischen hybriden Taktiken bedrohen direkt und unmittelbar zentrale Sicherheitsinteressen der EU und Österreichs.

Inhaltsverzeichnis

1. Einleitung und Begriffserklärung

Die hybride Kriegsführung ist im Prinzip kein neues Phänomen. Aus strategischer Sicht war der Einsatz von Mitteln, die zwar nicht zu den konventionellen kriegerischen gehören aber dennoch politische Interessen verfolgen bzw. militärische Ziele begünstigen, seit jeher eine beliebte Methode, um Einfluss, Macht oder Kontrolle auszuüben. Spuren dieser Strategien finden sich selbst in Sun Tzus zeitlosen Werk „Die Kunst des Krieges“ wieder, wenn vom Einsatz von Spionen und Sabotageakten die Rede ist. Betrachtet man die dahinterliegenden Intentionen, kann daher davon ausgegangen werden, dass die Anwendung hybrider Aspekte der Kriegsführung damals wie heute auf denselben Beweggründen beruht: den Gegner mittels nicht (klassisch) militärischen Instrumenten zu schwächen, Angriffe zu tarnen und unterhalb der Schwelle des Krieges größtmöglichen Schaden zuzufügen. Zwar haben sich die Absichten der hybriden Kriegsführung bzw. Einflussnahme über die letzten Jahrhunderte nur unwesentlich verändert, die modernen hochtechnologisierten Mittel und Wege zur Planung und Ausführung solcher Angriffe sind jedoch unvergleichbar komplexer. Dies wird durch die gängigen Definitionen von hybriden Bedrohungen und ihren Charakteristiken verdeutlicht.

Hybride Bedrohungen charakterisieren sich durch den koordinierten Einsatz verschiedener Methoden der illegitimen Einflussnahme (diplomatische, militärische, wirtschaftliche oder technologische) vonseiten staatlicher und nicht-staatlicher Akteure, ohne dass die Schwelle eines offiziell erklärten Krieges erreicht wird. Beispiele hierfür sind die Behinderung demokratischer Entscheidungsprozesse durch massive Desinformationskampagnen, die Nutzung sozialer Medien zur Kontrolle des politischen Narrativs oder zur Radikalisierung, Rekrutierung und Steuerung von stellvertretenden Akteuren.[1]

Definition von hybriden Bedrohungen des Bundesministeriums für Europäische und internationale Angelegenheiten (Österreich).

In modernen Konfliktszenarien setzen Angreifer auf eine Kombination aus klassischen Militäreinsätzen, wirtschaftlichem Druck, Computerangriffen bis hin zu Propaganda in den Medien und sozialen Netzwerken. Dieses Vorgehen wird auch als „hybride Taktik“ oder „hybride Kriegsführung“ bezeichnet.[2]

Definition von hybriden Bedrohungen des Bundesministeriums der Verteidigung (Deutschland)

The term hybrid threat refers to an action conducted by state or non-state actors, whose goal is to undermine or harm a target by influencing its decision-making at the local, regional, state or institutional level. Such actions are coordinated and synchronized and deliberately target democratic states' and

institutions' vulnerabilities. Activities can take place, for example, in the political, economic, military, civil or information domains. They are conducted using a wide range of means and designed to remain below the threshold of detection and attribution.[3]

Definition von hybriden Bedrohungen des European Hybrid Centre of Excellence for Countering Hybrid Threats

Trotz einer fehlenden universellen Definition sind wesentliche Gemeinsamkeiten in den Begriffserklärungen von hybriden Bedrohungen erkennbar, aus welchen Rückschlüsse auf die Eigenschaften der hybriden Natur jener Angriffe gezogen werden können. Diese zentralen Aspekte umfassen folgende Merkmale:

- Hybride Angriffe können von staatlichen oder nichtstaatlichen Akteuren, bzw. einer Verschmelzung beider Gruppen, ausgehen. Eine eindeutige Rückverfolgung von Angriffen ist meistens nicht möglich, die Verschleierung des Ursprungs der Angriffe ist charakteristisch.
- Hybride Angriffe verbinden und synchronisieren klassisch militärische Elemente mit illegitimer Einflussnahme in nicht-militärischen Domänen, wie u.a. durch wirtschaftliche, politisch/diplomatische, technologische oder mediale Methoden.
- Hybride Angriffe treten nicht zufällig auf, sie werden aufeinander abgestimmt und systematisch durchgeführt, indem gezielt die Schwachstellen von (demokratischen) Staaten, Institutionen und Gesellschaften anvisiert werden.
- Moderne technologische Mittel, insbesondere im Bereich der Informationstechnologie, werden für die Entwicklung und Durchführung von hybriden Angriffen herangezogen. Dies gilt speziell für Cyberangriffe und Desinformationskampagnen, welche die gängigsten hybriden Angriffsmethoden darstellen.

2. Die russische hybride Kriegsführung

Im Kontext der russischen Militärdoktrin stellt die hybride Kriegsführung ein klar definiertes Konzept dar. Der hybride Krieg wird als strategische Maßnahme zur Einflussausübung auf Regierungen sowie Irreführung von Bevölkerungen angesehen. Anders als im westlichen Diskurs und Verständnis beschreibt der hybride Krieg gemäß der Auffassung russischer Militärstrategie nicht ausschließlich die angewandten Mittel und Methoden, sondern stellt eine eigene Kategorie von Krieg dar.[4] Daher ist die US-amerikanische und europäische gängige Auslegung, dass sich die hybride Kriegsführung in einem „Graubereich" zwischen einem klar abgrenzbaren Kriegs- und Friedenszustand einordnen lässt, nicht mit der russischen Interpretation vereinbar. Denn aus russischer Sicht werden auch in Zeiten ohne direkte militärische Konfrontation kriegerische Intentionen und Handlungen durch unkonventionelle Mittel auf der kategorischen Ebene des hybriden Kriegs verfolgt. Es ist vor diesem Hintergrund unerlässlich, die strategischen Konzepte und taktischen Umsetzungen der hybriden Kriegsführung aus russischer Perspektive zu analysieren und begreifen, um daraus abgeleitet Schlüsse für die sich verändernde Sicherheitslage in Europa zu ziehen.

In diesem Zusammenhang ist ein weiterer Aspekt von zentraler Bedeutung: In der russischen Auslegung steht die Informationskampagne (Beherrschung eines bestimmten Narrativs) an höchster Stelle, alle anderen hybriden Angriffe, bis hin zum Einsatz von konventionellen Streitkräften, sind diesem Prinzip untergeordnet.[5] Einen staatlich kontrollierten Wahrheitsanspruch zu propagieren war bereits in der Sowjetunion eine weitverbreitete Ambition, welche sich, um nur ein Beispiel zu nennen, in der versuchten Vertuschung und Verharmlosung der Nuklearkatastrophe von Tschernobyl widerspiegelt.

Im heutigen Kontext wird Russlands „Militarisierung" von Information durch den Einsatz der Staatsmedien im Ausland verdeutlicht. Die Chefredakteurin des Auslandssender RT (ehemals Russia Today), mit globaler Reichweite nannte den Sender bereits 2013 eine „Informationswaffe", welche Russland im „Informationskrieg" nutzen kann, um das Publikum

für russische Zwecke zu „erobern“ und Parallelgesellschaften zu schaffen.[6] Die russische staatliche Nachrichtenagentur Rossija Sewodnja, welche neben RT und Sputnik auch eine Vielzahl anderer Sender und Kanäle betreibt und weltweit Millionen von Menschen erreicht, wurde per Dekret vom Kreml ins Leben gerufen, mit dem Ziel, über die staatlichen Politikinteressen zu berichten.[7] Obwohl sich diese Plattformen sowohl im Aussehen als auch in der Selbstdarstellung geschickt als vermeintlich seriöse Nachrichtenagenturen tarnen, können sie aufgrund ihrer staatlichen Finanzierung, ihrer Zielausrichtung und ihres Einsatzes nicht mit herkömmlichen Sendern vergleichen werden, sondern müssen als Manipulationseinrichtungen des Kremls angesehen werden. Darüber hinaus stellen die russischen Cyber-Akteure eine signifikante Rolle in den Informationsoperationen und der hybriden Kriegsführung dar. Durch den konstanten Ausbau von Cyber-Kapazitäten wurde Russland zu einem führenden Aggressor im digitalen Raum und hob damit den Stellenwert der Cyber-Kriegsführung auf eine Ebene mit konventionellen militärischen Fähigkeiten.[8]

Laut den Analysen des US-Außenministeriums baut das russische Desinformations- und Propaganda-Ökosystem auf fünf zentralen Säulen auf: (1) die offizielle Kommunikation des Kremls, (2) vom Staat finanzierte globale Nachrichtenübermittlung, (3) den Aufbau von Proxy-Netzwerken, (4) die Instrumentalisierung von Sozialen Medien als Waffe und (5) durch Cyberangriffe forcierte Desinformation.[9] Dabei sind folgende Ableitungen wesentlich für das tiefergreifende Verständnis der russischen hybriden Kriegsführung:

- Es ist ein vom Kreml ausgehender Top-Down-Ansatz erkennbar, denn die erste Säule baut auf den anderen auf. Die vom Kreml vorgegebene Kommunikation ist somit mittels hybrider Mittel zu verbreiten.
- Staatliche Nachrichtensender wie RT und Sputnik, aber auch die Desinformationskampagnen auf den Sozialen Medien, welche durch Troll-Fabriken mit direkten Verbindungen zum russischen Auslandsmilitärgeheimdienst (GRU) erstellt und gestreut werden,[10] sind Multiplikatoren der Kreml-gesteuerten Narrative. Dazu gehören auch die weitreichenden russischen Einfluss-Netzwerke in politische Parteien in Europa.[11]
- Die gezielte Synchronisation von verschiedenen hybriden Angriffen und Manipulationsmethoden wird in dieser Struktur evident. Sowohl Cyberangriffe als auch Desinformationskampagnen werden als Mittel zum Zweck gesehen, um das öffentliche Meinungsbild zu kontrollieren.
- Das dargestellte Ökosystem wirkt sowohl nach Außen (insbesondere zur Erweiterung des subversiven Einflusses auf Europa) als auch nach Innen (zur Kontrolle der Opposition bzw. des öffentlichen Diskurses innerhalb Russlands).

Abbildung 1 - Die fünf Säulen des russischen Desinformations- und Propaganda-Ökosystems (U.S. Department of State. Global Engagement Center (GEC) 2022)

3. Russische Einflussausübung in Post-Sowjet-Staaten durch hybride Instrumente

Bereits vor dem 24. Februar 2022 bestand kein Zweifel daran, dass Russlands hybride Taktiken im Post-Sowjet-Raum auf die Destabilisierung der Europa- bzw. westlich-orientierten Bevölkerungen und Regierungen abzielt, um den eigenen Einfluss (auf militärischer, politischer, und wirtschaftlicher Ebene) in jenen Ländern auszubauen. Die Länder der ehemaligen Sowjetunion, im russischen Kontext auch „nahes Ausland" genannt, sind das wichtigste Einflussgebiet Russlands. Die konstante Machtprojektion und Einflussausübung des Kremls in postsowjetischen Staaten stellt somit eine zentrale innen- sowie außenpolitische Zielsetzung dar. Zudem wird an die russische Bevölkerung ein mystifizierter Symbolcharakter bestimmter Regionen und Gebiete in jenen Ländern propagiert, welche identitätsstiftend wirken sollen und somit die politischen und militärischen Handlungen zu legitimieren versucht. Dies trifft speziell für den Donbass zu, wie die Wiederbelebung von Propagandaslogans wie „Donbass ist das Herz Russlands", die an die 1920er Jahre erinnern lassen, verdeutlichen.[12]

Die großrussischen Ambitionen werden insbesondere durch die Analyse der hybriden Einflussnahme evident, da diese sich nicht nur auf die Ukraine beschränken. Transnistrien, ein bedeutender Industriestandort während der Sowjetunion, im heutigen Moldawien, steht seit Anfang der 1990er Jahre politisch und militärisch unter dem Einfluss von Russland – die jahrzehntelange Militärpräsenz von ca. 1.500 russischen Soldaten bekräftigt die Positionierung Russlands symbolisch und reell.[13] Die abtrünnigen Gebiete Abchasien und Südossetien in Georgien werden von Russland als unabhängige Staaten angesehen und unterliegen massiver russischer Kontrolle. Die autoritäre Regierung in Belarus ist politisch und ökonomisch in enormem Ausmaß von Russland abhängig – der Umgang mit den großflächigen Protesten im Zuge der Präsidentschaftswahlen 2020 verstärkte die Tatsache, dass das politische Überleben von Präsident *Lukashenko* an die russische Unterstützung gebunden ist.[14] Das von Russland angeführte Militärbündnis, die Organisation des Vertrags über kollektive Sicherheit, welcher sechs ehemalige Sowjetrepubliken angehören, entsandte im Zuge der Proteste in Kasachstan erstmalig „Friedenstruppen", um den von Russland porträtierten „vom Ausland unterstützen Terroristen-Aufstand" niederzuschlagen.[15]

Auf all diese Fälle im Detail einzugehen, würden den Rahmen der vorliegenden AIES Kurzstudie sprengen. Dennoch ist signifikant, dass sich Russland in seiner Einflussausübung stets hybrider Maßnahmen bedient. Die Kombination und Synchronisation von klassisch militärischen und nicht-militärischen Instrumenten ist hierbei klar erkennbar, genauso wie der Umstand, dass der Kreml in der Verfolgung seiner Ambitionen keine Verstöße gegen das humanitäre Völkerrecht oder die regelbasierte internationale Ordnung scheut.

4. Russische hybride Kriegsführung im Kontext des Angriffskriegs auf die Ukraine

Die russische hybride Kriegsführung gegen die Ukraine ist beispiellos; weder die Intensität noch das Ausmaß der Angriffe wird von anderen Fällen übertroffen. Besonders deutlich und zahlreich waren die hybriden Elemente im Zuge der Annexion der Krim und der Destabilisierung der Ostukraine 2014, als eine systematische Vermischung konventioneller Kriegsführung mit irregulären Kämpfern, verdeckten Operationen, Infiltrationen und militärischer Unterstützung von Separatisten zur Anwendung kam.[16] Jedoch lassen sich auch hybride Aspekte der Einflussnahme vor 2014 identifizieren, wie unter anderem die vermeintlich von Russland ausgeübte Vergiftung von Viktor Juschtschenko 2004. Seit 2014 kam es zudem laufend zu geschichtsverzerrenden Desinformationskampagnen und großflächigen Cyberangriffen, teilweise mit globalen Auswirkungen, wie die Petya und NotPetya Angriffe 2017 und 2018 gezeigt haben.

Ohne auf die gut dokumentierten Details jener Ereignisse einzugehen, soll an dieser Stelle erwähnt werden, dass sich bereits seit 20 Jahren eine kontinuier-

lich stattfindende hybride Einflussnahme Russlands auf die Ukraine nachvollziehen lässt, die stetig an Wirkung zugenommen hat. Insbesondere hinsichtlich des russischen Ziels, die Informationshoheit über die Ukraine-Narrative zu erlangen, führte der Kreml zahlreiche erfolgreiche Informationskampagnen durch, vor allem im Kontext der Minsk-II-Vereinbarungen, in welchen Deutschland und Frankreich Russland als Vermittler und nicht als Kriegspartei in der Ukraine akzeptierten.[17]

Der Fokus dieser AIES Kurzstudie liegt auf dem Zeitraum von Anfang 2022 bis Anfang 2023, in welchem sich die russischen hybriden Kriegstaktiken im Kontext des Angriffskriegs auf die Ukraine zugespitzt haben. Dabei liegt der Schwerpunkt auf der Analyse der markantesten Arten der russischen hybriden Kriegsführung gegen die Ukraine: Cyberangriffe und Desinformationskampagnen

Russische Cyberangriffe im Zusammenhang des Angriffskriegs auf die Ukraine

Die russischen Cyberangriffe auf die Ukraine nahmen bereits einige Wochen vor Beginn der militärischen Invasion am 24. Februar 2022 stetig zu und können aus strategischer Sicht als Vorboten des klassischen militärischen Angriffs gesehen werden. Während die diplomatischen Bemühungen zwischen Russland, den USA, und der Ukraine im Jänner 2022 keine Erfolge erzielten und sich die russische Truppenmobilisierung entlang der ukrainischen Grenze in Vorbereitung der Invasion abzeichnete, griffen russische Cyber-Gruppen die Ukraine bereits mit erhöhter Intensität an.[18] Mittels Schadsoftware, die auf die Vernichtung von sensiblen Daten innerhalb ukrainischer Regierungsbehörden abzielte, wurde eine destruktive Phase an Cyberangriffen gegen die Ukraine eingeleitet. Zu den gängigsten digitalen Angriffstypen zählten insbesondere „distributed denial of service“ (DDoS) Attacken gegen Webseiten der Regierung sowie den IT-, Energie-, Kommunikations- und Finanzsektor. Somit wurden die russischen Cyberangriffe auf die Ukraine in den Wochen vor Beginn der Invasion als vorbereitende Maßnahmen eingeleitet, welche die Handlungsfähigkeit der ukrainischen Regierung schwächen sowie Schlüsselsektoren schädigen sollten.

Darüber hinaus kam es in den Tagen und Stunden vor dem Militärangriff zu gezielten digitalen Attacken auf kritische Infrastruktur, Medien und Kommunikationsnetzwerke. Dazu zählten unter anderem die Cyberangriffe auf die kritische Infrastruktur in Odessa und Sumy sowie gegen die Nachrichtenagentur Kyiv Post.[19] Besonders weitreichend war der Angriff auf das Viasat KA-SAT Satelliten Netzwerk, wenige Stunden vor Beginn der Invasion am 24. Februar 2022. Dieser Cyberangriff legte die satellitengesteuerte Breitbandinternetverbindung lahm und schränkte somit nicht nur die militärischen Telekommunikationsnetzwerke der Ukraine ein, sondern kappte auch den Internetzugang für die Zivilbevölkerung.[20] Der Cyberangriff auf Viasat verursachte auch Schäden für EU-Mitgliedsstaaten. Ein deutsches Energieunternehmen verlor den Fernüberwachungszugang zu

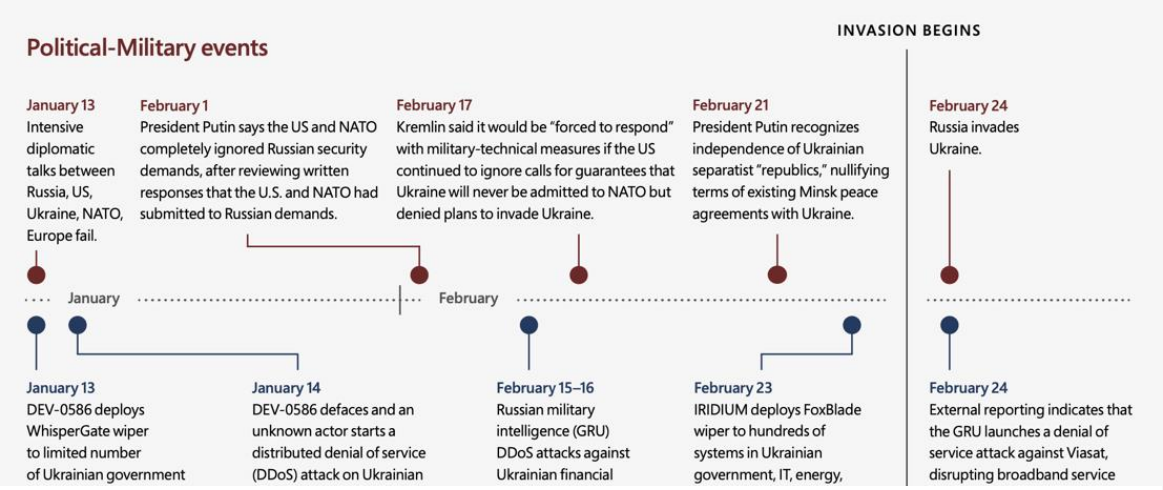

Abbildung 2 – Politisch-militärische Entwicklungen und Cyberangriffe Jänner/Februar 2022 (Microsoft Digital Security Unit 2022)

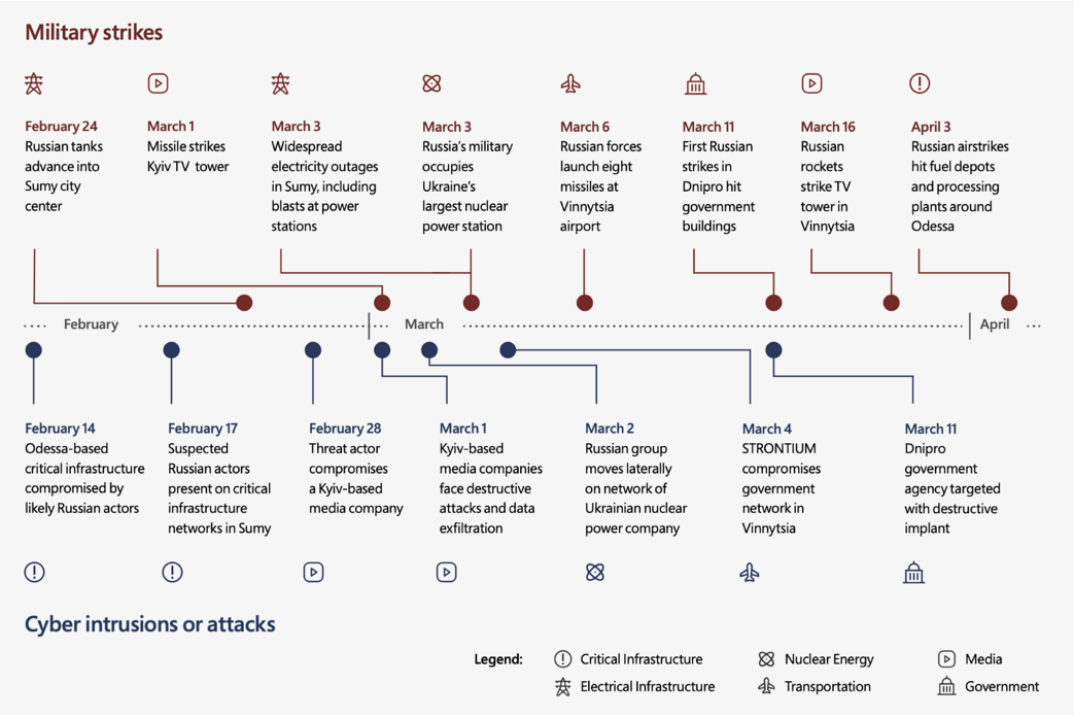

Abbildung 3 – Synchronisation von Militärschlägen und Cyberangriffen Februar – April 2022 (Microsoft Digital Security Unit 2022)

mehr als 5.800 Windturbinen, knapp 9.000 Abonnent:innen eines französischen Internetdienstleisters waren von Ausfällen betroffen und insgesamt hatten zehntausende Festnetz-Breitbandkund:innen eingeschränkten Internetzugang.[21]

Bei der Analyse russischer Militärschläge und Cyberangriffe zeigen mehrere, zeitlich aufeinander abgestimmte, Beispiele eine Koordinierung von digitalen Operationen und militärischen Angriffen. In mehreren Fällen gingen Angriffe auf Computernetzwerke einem unmittelbaren Militärschlag voraus, was auf eine Synchronisation der Angriffe hindeutet. Somit kann davon ausgegangen werden, dass die russischen Cyber-Operationen im Einklang mit Maßnahmen standen, die darauf abzielten, die ukrainischen Regierungs-, Militär- und Wirtschaftsfunktionen zu beeinträchtigen, zu stören oder zu diskreditieren, kritische Infrastruktur zu unterbrechen und den Zugang der ukrainischen Öffentlichkeit zu Informationen einzuschränken.[22]

Die Zeitleiste der Militärschläge und Cyberangriffe zeigt demnach nicht nur die Synchronisation von konventionellen und hybriden Kriegstaktiken, sondern auch, dass aus Sicht des Angreifers militärisch offensive Vorstöße und digitale Mittel dieselben Kriegsziele verfolgen. Während jedoch die konventionellen Angriffe auf dem Schlachtfeld durch physikalische Gesetzmäßigkeiten bestimmt werden, können Cyberangriffe digitale Einrichtungen weit hinter den Frontlinien infiltrieren und beschädigen, und decken ein breiteres Spektrum an möglichen militärstrategisch wichtigen Zielen ab.

Trotz des hohen Niveaus und der technischen Raffinesse der Cyberangriffe ist es bei genauerer digitalforensischer Untersuchung möglich den Spuren der Angreifer zu folgen und die direkte Beteiligung verschiedener staatlicher Stellen nachzuweisen. Durch die Beobachtung und Analyse der Cyber-Aktivitäten von einigen der berüchtigtsten russischen Akteure konnten, mithilfe von Berichten aus der Vergangenheit,[23] die verantwortlichen Hackergruppen sowie deren Verbindungen zu russischen Geheimdiensten identifiziert werden.[24] Zu den professionellsten Cyber-Gruppen, die für den Großteil an schwerwiegenden russischen Cyberangriffen im Zeitraum von Februar bis Juni 2022 verantwortlich waren, zählen unter anderem Sandworm, APT28, und InvisiMole. Die Analyse von Trustwave, dargestellt durch die Zeitachse und Grafik auf den nächsten Seiten, konnte die Verbindungen dieser Gruppen zu speziellen Einheiten des russischen Militärgeheimdiensts GRU sowie zum Inlandsgeheimdienst

FSB nachweisen, während andere Angriffe auch dem Dienst der Außenaufklärung SVR zugeordnet werden können.[25] Die direkte Verbindung der Cyber-Gruppen zu verschiedenen russischen staatlichen Diensten kann laut diesen Quellen daher ohne Zweifel bestätigt werden.

Russische Desinformation im Zusammenhang des Angriffskriegs auf die Ukraine

Nur wenige Tage nach Beginn des Angriffskriegs beschloss die Europäische Union die Sendeaktivitäten der russischen Staatsmedien innerhalb der EU einzustellen, um die russische Desinformation und Informationsmanipulation über den Angriff einzudämmen. Der Hohe Vertreter der EU für Außen- und Sicherheitspolitik Josep Borrell fand in diesem Zusammenhang sehr klare Worte. Er identifizierte die systematischen Desinformationskampagnen des Kremls als operatives Instrument der russischen Kriegsführung gegen die Ukraine sowie als signifikante und direkte Bedrohung der Sicherheit und öffentlichen Ordnung der EU und ihrer Mitgliedsstaaten.[26]

Russland bereitete jedoch bereits vor der militärischen Invasion seinen geplanten Angriffskrieg mittels der Erstellung und Verbreitung von Desinformation vor. Durch gezielte Falschmeldungen zu den angeblichen Hintergründen, dem vorbereiteten Angriff selbst sowie der Legitimation der Aggression versuchte der Kreml den Weg für den militärischen Überfall über die Kontrolle der Narrative zu ebenen. In dieser Phase wurden folgende Desinformationsnarrative vordergründig eingesetzt:[27]

„Russland und die Ukraine sind eine Nation“

Diese manipulative Darstellung ist eines der ältesten und in russischen Medien weitverbreitetsten Narrative mit dem subversiven Zweck, der Ukraine ihr Existenzrecht und ihre Souveränität zu entziehen.[28] Seit der russischen Annexion der Krim 2014 wird dieser Mythos gezüchtet, um die russischen Gebietsansprüche in der Ukraine zu rechtfertigen. Die strategische Missinterpretation historischer Ereignisse gegenüber der russischen Bevölkerung sowie die kulturell-ideologische Prägung der „Rückkehr der Ukraine in die (russisch) kulturelle Heimat“ sind in diesem Kontext besonders dominant.

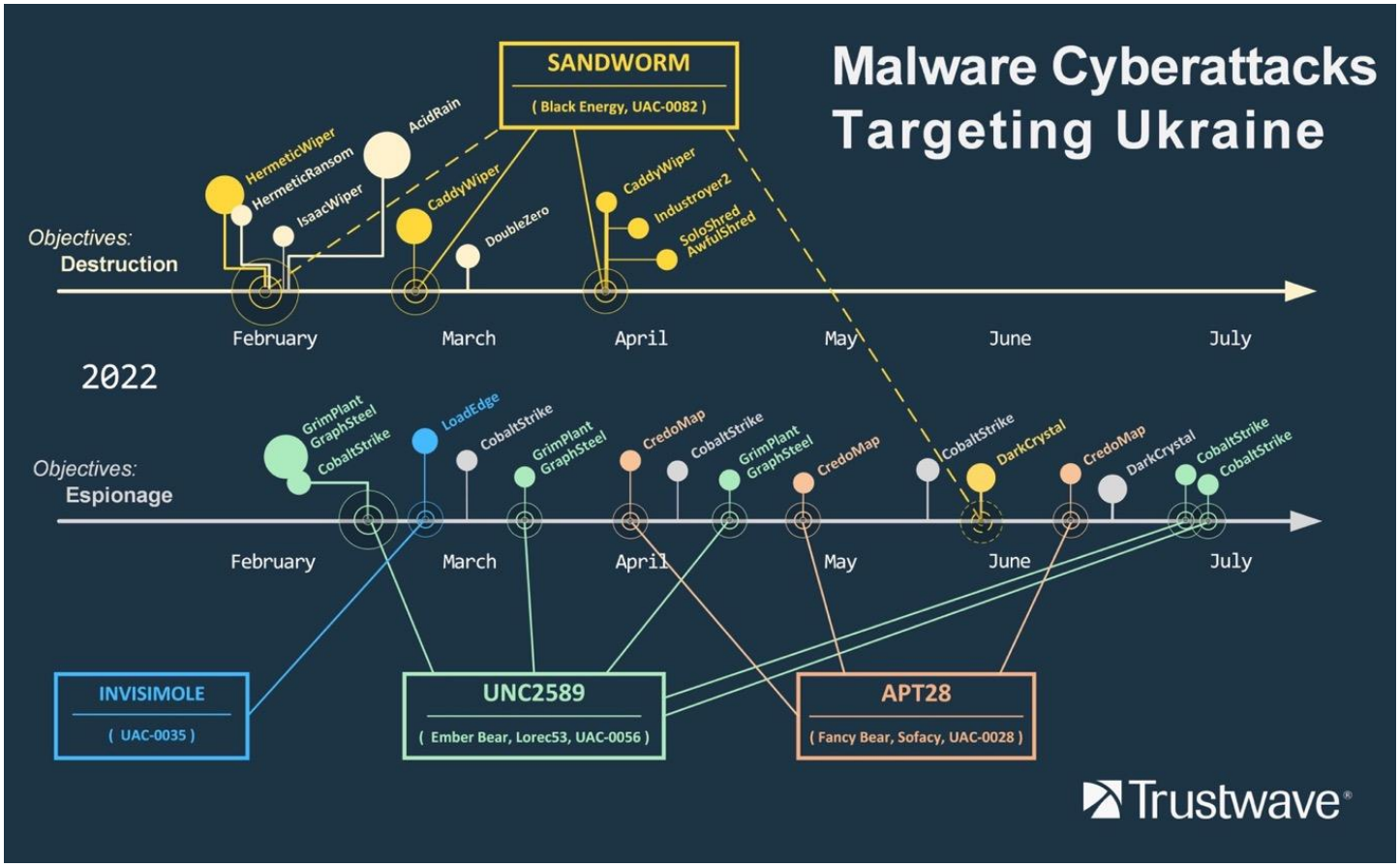

Abbildung 4 – Malware Cyberangriffe auf die Ukraine, 2022 (Knapczyk 2022)

Abbildung 5 – Russische Cyber-Gruppen und deren Verbindung zu den Geheimdiensten29F (Knapczyk 2022)

„Die russischsprachige Bevölkerung im Donbass ist Gräueltaten ausgesetzt“

Durch fälschliche Anschuldigungen, dass es im Osten der Ukraine zum Genozid an russischsprachigen Bürger:innen kommen würde, versuchte der Kreml die russische Bevölkerung für den Krieg zu mobilisieren und Legitimität aufzubauen. Dieses Narrativ wurde durch emotionalisierte Falschmeldungen weiter befeuert, wie unter anderem die erfundene Geschichte von einem gekreuzigten Jungen in der Ostukraine, die seit 2014 immer wieder von russischen Medien als Referenzpunkt für angeblichen Völkermord hergenommen wurde.[29]

„Russland führt keinen Angriffskrieg, sondern eine ‚Spezialoperation‘ zur Entnazifizierung der Ukraine“

Das Desinformationsnarrativ, die Ukraine sei durch Faschisten bzw. Nazis beherrscht, ist in den russischen Staatsmedien ebenfalls sehr prominent. Hierbei bedient sich die russische Führung komplett verfälschter historischer Bezugspunkte und schürt alte Feindbilder zur Delegitimierung der ukrainischen politischen Führung. Hierbei ist ebenfalls eine konstant steigende Wiederholung der Falschdarstellungen seit 2014 erkennbar.[30] Die Begriffe „Faschisten“ oder „Nazis“ werden darüber hinaus nicht nur ungeachtet des historischen Kontexts synonym verwendet, sondern richten sich undifferenziert als generelle Anschuldigung gegen all jene Staaten, die der Ukraine Hilfeleistungen im Krieg gegen Russland zugesichert haben.[31] Darüber hinaus wurde der Angriffskrieg bis heute als „Spezialoperation“ heruntergespielt, um speziell der eigenen Bevölkerung gegenüber das Ausmaß des Krieges vorzuenthalten.

Trotz der russischen Bemühungen diese Narrative über den Angriffskrieg nicht nur innerhalb der russischen, sondern auch innerhalb der europäischen Gesellschaft zu streuen, ist letzteres durch die Maßnahmen der EU zur Einschränkung russischer Desinformation und zur Aufklärung der Bevölkerung nur sehr beschränkt gelungen. Russland hat demnach die Zielsetzung der Informationsoperationen vor Beginn des Angriffskriegs nur begrenzt erreicht. Dennoch hat Russland im weiteren Verlauf des Angriffskriegs Informationsoperationen als strategisches Mittel verwendet, um militärische Ziele zu erreichen. In den folgenden Fällen lässt sich eine besonders enge Verflechtung von Desinformationskampagnen und militärstrategischen Zielen erkennen:

Die russischen Desinformationskampagnen gegen die Europäische Union (und die USA) verfolgten das strategische Ziel die europäische Solidarität zu brechen und die materielle Unterstützung der Ukraine zu verhindern bzw. zu verlangsamen.[32]

Russland erkannte, dass die ukrainische Widerstandsfähigkeit stärker ist als ursprünglich angenommen und dass die russischen Streitkräfte nicht in der Lage waren entscheidende Siege zu verzeichnen. Durch die europäische und westliche Unterstützung gestärkt, gelang es hingegen der Ukraine militärische Erfolge zu erzielen und besetzte Gebiete von russischen Truppen zu befreien. Um der westlich/europäischen Unterstützung entgegenzuwirken und den militärischen Widerstand so gering wie möglich zu halten, schürte der Kreml durch Desinformation gezielt Ängste innerhalb der europäischen Bevölkerung. Dieses Ziel manifestierte sich durch verschiedene Narrative. Einerseits wurden verehrende Wirtschaftskrisen für Europa prognostiziert und der Einsatz von Atomwaffen angedroht.[33] Andererseits wurden Falschmeldungen über geflüchtete Personen aus der Ukraine verbreitet, um die Migrationsdebatte zu instrumentalisieren und Geflüchtete zu dämonisieren.[34] Wie emotionalisiert diese Informationsoperationen sind, zeigt insbesondere die Verbreitung von Falschmeldungen über ukrainische Geflüchtete, in welchen dargestellt wurde, dass wohlhabende Ukrainer:innen Sozialhilfe in Europa erhalten haben oder dass es zu gewaltvollen Ausschreitungen gegen die europäische Bevölkerung gekommen sei.[35] Somit wird versucht durch die strategische Verbreitung von Desinformation operative Militärziele am Schlachtfeld zu begünstigen.

Die russischen Desinformationskampagnen versuchen eigne militärische Misserfolge abzumildern bzw. die Voraussetzungen für geplante Operationen zu schaffen.[36]

Bei jener Art von Desinformationskampagnen steht die Demoralisierung der ukrainischen Bevölkerung stark im Vordergrund, indem der Versuch unternommen wird, den Kampfeswillen und dadurch die Widerstandsfähigkeit der Ukraine zu brechen. Dies findet auf verschiedenen Narrativ-Ebenen statt. Zum einen werden die russischen militärischen Fähigkeiten besser dargestellt als sie in Wirklichkeit sind. Das soll die russische Machtprojektion und Abschreckung bestärken – auch in Richtung Europa.[37] Zum anderen soll der falsche Eindruck vermittelt werden, dass die Ukraine nicht in der Lage ist die russischen Angriffe abzuwehren bzw. dass die ukrainische Führung kurz vor der Kapitulation stehen würde. Ein markantes Beispiel dafür, welches auch die Gefahrenpotenziale hochmoderner technologischer Möglichkeiten aufzeigt, sind Deepfakes: unechtes Video- und Tonmaterial, dass oftmals mittels „Künstlicher Intelligenz“ erstellt wird und auf den ersten Blick kaum als Attrappe identifiziert werden kann. Bereits Anfang März 2022 kursierten täuschend echte Deepfake-Videos des ukrainischen Präsidenten Selenskyj, in welchen die Soldaten aufgerufen werden ihre Waffen niederzulegen und zurück zu ihren Familien zu gehen.[38] Neue digitale Programme, wie unter anderem Midjourney, ermöglichen es mit sehr geringem Aufwand und überschaubaren IT-Wissen verfälsche Videos und Bilder mit erstaunlicher Qualität spielendleicht zu generieren, was Informationsoperationen neue Dimensionen der Manipulation eröffnet. In weiteren Fällen von Operationen mit direktem Draht zur GRU wurde fälschlicherweise behauptet Präsident Selenskyj hätte in einem Bunker Selbstmord begangen, um das Militär und die Bevölkerung zu demoralisieren, um günstige Voraussetzungen für russische Angriffe zu schaffen.[39]

Dass sich im Kontext des russischen Angriffskriegs auf die Ukraine das Schlachtfeld auch auf der digitalen Informationsebene abspielt, wird somit evident. Russland wird auch im weiteren Kriegsverlauf Informationsoperationen als Waffe einsetzten, um die militärischen Zielsetzungen direkt zu begünstigen, die eigenen Misserfolge zu verschleiern, die Ukrainer:innen moralisch zu schwächen und Drohkulissen gegenüber dem Westen zu inszenieren. Im Kern unterstützen diese Informationsoperationen auch das übergeordnete strategische Ziel des Kremls, die Ukraine militärisch vom Westen zu isolieren und die Europäische Union in ihrem politischen und gesellschaftlichen Zusammenhalt sowie in der Unterstützung der Ukraine zu untergraben.[40]

5. Conclusio

Aus der Analyse und Beobachtung der russischen Kriegsführung gegen die Ukraine, mit Schwerpunkt auf den Zeitraum seit 24. Februar 2022, geht klar hervor, dass Russland hybride Angriffselemente zur Erfüllung von militärischen Zielen anwendet. Die Professionalität, Reichweite und Intensität der hybriden Angriffe sowie die Synchronisation mit konventionellen Methoden zeigt, dass hybride Mittel bereits gänzlich ins Arsenal der russischen Kriegsführung integriert sind. Ungeachtet ihrer direkten oder indirekten Letalität, stellen insbesondere Cyberangriffe und Desinformationskampagnen gängige Waffen im russischen Angriffskrieg gegen die Ukraine dar. Durch die Möglichkeit Schwachstellen in demokratischen Systemen und pluralistischen Gesellschaften auszunutzen, die eigene Bevölkerung durch emotionalisierte und systematisch kultivierte Narrative zu mobilisieren und gleichzeitig offensive Kriegsgeschehnisse zu legitimieren sowie die Spuren und Ursprünge von digitalen Angriffen zu verschleiern, haben sich hybride Kriegstaktiken als effektive und effiziente Aggressionsausübung etabliert. Russland hat somit gelernt, dass zur Durchsetzung seiner militärischen und politischen Interessen hybride Angriffsmethoden attraktive Alternativen und Ergänzungen zu klassisch militärischen Mitteln sind. Wie russische Cyberangriffe und Desinformationskampagnen zeigen, wird dabei nicht nur die Ukraine angegriffen, sondern auch die Europäische Union und ihre Mitgliedsstaaten.

About the Author

Michael Zinkanell, M.A./B.A., ist Direktor des Austria Instituts für Europa- und Sicherheitspolitik (AIES). Neben seiner Expertise in europäischer Sicherheits- und Verteidigungspolitik sowie geopolitischen Entwicklungen liegt sein analytischer Schwerpunkt auf der Analyse der sicherheitspolitischen Implikationen von hybriden Bedrohungen, Desinformationskampagnen und Cyberattacken.

[1] BMEIA. 2023. „Hybride Bedrohungen.“ Abgerufen am 20. Februar 2023. https://www.bmeia.gv.at/themen/globale-themen/hybride-bedrohungen/.

[2] BMVG. 2023. „Was sind hybride Bedrohungen.“ Abgerufen am 03.März 2023. https://www.bmvg.de/de/themen/sicherheitspolitik/hybride-bedrohungen/was-sind-hybride-bedrohungen—13692.

[3] Hybrid CoE. 2023. „Hybrid threats as a concept.“ Abgerufen am 05. März 2023. https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/.

[4] Clark, Mason. 2020. „Russian Hybrid Warfare.” Military Learning and the Future of War Series, September; abgerufen am 03. März 2023. https://www.understandingwar.org/report/russian-hybrid-warfare.

[5] Ibid.

[6] EUvsDISINFO. 2022. „Die Manipulationskanäle des Kremls: Sieben Dinge, die Sie über RT und Sputnik wissen sollten.“ EUvsDISINFO, 4. März; abgerufen am 24. Februar 2023. https://EUvsDiSiNFO.eu/de/die-luegenkanaele-des-kremls-sieben-dinge-die-sie-ueber-rt-und-sputnik-wissen-sollten/.

[7] U.S. Department of State. Global Engagement Center (GEC). 2022. „RT und Sputnik und ihre Rolle im russischen Desinformations- und Propaganda-Ökosystem.“ GEC-Sonderbericht, Jänner; abgerufen am 24. Februar 2023. https://www.state.gov/wp-content/uploads/2022/08/DE_Kremlin-Funded-Media_January_update-19.pdf.

[8] Välisluureamet (Estonia Foreign Intelligence Service). 2018. „International Security and Estonia 2018.“ Abgerufen am 20. Jänner 2023. https://valisluureamet.ee/doc/raport/2018-en.pdf.

[9] U.S. Department of State. Global Engagement Center (GEC) 2022

[10] EUvsDISINFO. 2019. “’Information War’ is a Term used by the Kremlin to justify Disinformation.” EUvsDISINFO, 22. Oktober; abgerufen am 19. Februar 2023. https://EUvsDiSiNFO.eu/information-war-is-a-term-used-by-the-kremlin-to-justify-disinformation/.

[11] Polyakova, Alina, Flemming Splidsboel Hansen, Robert Van der Noordaa, Øystein Bogen und Henrik Sundbom. 2018. „The Kremlin´s Trojan Horses.“ Atlantic Council, 4 Dezember; abgerufen am 16. Februar 2023. https://www.atlanticcouncil.org/wp-content/uploads/2021/02/The-Kremlins-Trojan-Horses-3.pdf.

[12] Chalupa, Irena. 2014. „DIRECT TRANSLATION: ‘Donbas, the Heart of Russia’.“ Atlantic Council, 12. Juni; abgerufen am 05. März 2023. https://www.atlanticcouncil.org/blogs/new-atlanticist/direct-translation-donbas-the-heart-of-russia/.

[13] Solovyov, Vladimir. 2022. „Ukraine War Risks Repercussions for Transnistria.“ Carnegie, 23. September; abgerufen am 05. März 2023. https://carnegieendowment.org/politika/87986.

[14] Leukavets, Alla. 2021. „Russia’s game in Belarus: 2020 presidential elections as a checkmate for Lukashenka?“ New Perspectives 29 (1). https://journals.sage-pub.com/doi/10.1177/2336825X20984337.

[15] Watson. 2022. „Heftige Proteste in Kasachstan – Tote und über 1000 Verletzte, jetzt kommen die Russen.“ Watson, 06. Jänner; abgerufen am 13. März 2023. https://www.watson.ch/international/russland/962390297-proteste-in-kasachstan-eskalieren-russland-greift-ein.

[16] Tamminga, Oliver. 2015. „Hybride Kriegsführung: Zur Einordnung einer aktuellen Erscheinungsform des Krieges.“ SWP-Aktuell

27, 16. März; abgerufen am 20. März 2023. https://www.swp-berlin.org/publications/roducts/aktuell/2015A27_tga.pdf.

[17] Kagan, Frederick W. und Kateryna Stepanenko. 2023. "Russian Offensive Campaign Assessment.“ Institute for the Study of War; abgerufen am 17. März 2023. https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-february-12-2023.

[18] Microsoft Digital Security Unit. 2022. "An overview of Russia’s cyberattack activity in Ukraine.“ Abgerufen am 20. März 2023. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd.

[19] Przetacznik, Jakub. 2022. „Russia’s war on Ukraine: Timeline of cyber-attacks.“ European Parliament Think Tank, 21. Juni; abgerufen am 18. März 2023. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733549.

[20] Cyber Peace Institute. 2022.“Case Study.“ Abgerufen am 22. März 2023. https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat.

[21] Ibid.

[22] Microsoft Digital Security Unit 2022

[23] GOV UK. 2022. „Russia's FSB malign activity: factsheet.“ 5. April; abgerufen am 20. Februar 2023. https://www.gov.uk/government/publications/russias-fsb-malign-cyber-activity-factsheet/russias-fsb-malign-activity-factsheet.

[24] Knapczyk, Pawel. 2022. „Overview of the Cyber Weapons Used in the Ukraine - Russia War.“ SpiderLabs Blog, 18 August; abgerufen am 18. März 2023. https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war/.

[25] Ibid.

[26] Council of the EU. 2022. „EU imposes sanctions on state-owned outlets RT/Russia Today and Sputnik's broadcasting in the EU.“ 02. März; abgerufen am 23. März 2023. https://www.consilium.europa.eu/en/press/press-releases/2022/03/02/eu-imposes-sanctions-on-state-owned-outlets-rt-russia-today-and-sputnik-s-broadcasting-in-the-eu/.

[27] Delegation of the European Union to the People’s Republic of China. 2022. „Disinformation About Russia's invasion of Ukraine - Debunking Seven Myths spread by Russia“. 18. März; abgerufen am 23. März 2023. https://www.eeas.europa.eu/delegations/china/disinformation-about-russias-invasion-ukraine-debunking-seven-myths-spread-russia_en.

[28] Spahn, Susanne. 2023. „Nachrichten aus dem Kreml“. Bundeszentrale für politische Bildung, 12. Jänner; abgerufen am 23. März 2023. https://www.bpb.de/themen/medien-journalismus/digitale-desinformation/517057/nachrichten-aus-dem-kreml/.

[29] EUvsDISINFO. 2016. „Anniversary: "The crucified boy" turns two“. EUvsDISINFO, 15. Juli; abgerufen am 28. Februar 2023. https://euvsdisinfo.eu/anniversary-the-crucified-boy-turns-two/.

[30] Delegation of the European Union to the People’s Republic of China 2022

[31] Spahn 2023

[32] Kagan und Stepanenko 2023

[33] Spahn 2023

[34] ISD (Institute for Strategic Dialogue). 2022. „RUSSISCHE DESINFORMATION DÄMONISIERT UKRAINISCHE FLÜCHTLINGE.“ 08. Dezember; abgerufen am 20. März 2023. https://isdgermany.org/russische-desinformation-daemonisiert-ukrainische-fluechtlinge/.

[35] Neidhardt, Alberto-Horst und Paul Butcher. 2022. „Disinformation on Migration: How Lies, Half-Truths, and Mischaracterizations Spread.“ Migration Policy Institute, 8. September. Abgerufen am 20. März 2023. https://www.migrationpolicy.org/article/disinformation-migration-how-fake-news-spreads.

[36] Kagan und Stepanenko 2023

[37] Ibid.

[38] Milmo, Dan und Sauer, Pjotr. 2022. „Deepfakes v pre-bunking: is Russia losing the infowar?“ The Guardian, 19. März, abgerufen am 28. März 2023. https://www.theguardian.com/world/2022/mar/19/russia-ukraine-infowar-deepfakes.

[39] Wahlstrom, Alden, Revelli, Alice, Riddell Sam, Mainor David, Serabian Ryan. 2022. „The IO Offensive: Information Operations Surrounding the Russian Invasion of Ukraine“, Mandiant Blog, 19. Mai, abgerufen am 28. März 2023. https://www.mandiant.com/resources/blog/information-operations-surrounding-ukraine.

[40] Kagan und Stepanenko. 2023

Dr. Langweg 3, 2410 Hainburg/Donau

Tel. +43 (1) 3583080

office@aies.at | www.aies.at

Layout Design: Julia Drössler