MASTERARBEIT | MASTER'S THESIS

Titel | Title

Die Verteidigung europäischer Staaten gegen "Foreign Information Manipulation and Interference"

verfasst von | submitted by

Florian Höck BA BSc

angestrebter akademischer Grad | in partial fulfilment of the requirements for the degree of

Master of Arts (MA)

Wien | Vienna, 2025

Studienkennzahl lt. Studienblatt	Degree programme code as it appears on the student record sheet:	UA 066 824
Studienrichtung lt. Studienblatt	Degree programme as it appears on the student record sheet:	Masterstudium Politikwissenschaft
Betreut von	Supervisor:	Univ.-Prof. Dr. Patrick Müller Privatdoz. M.A.

Abstract

Diese Arbeit beschäftigt sich mit der Fragestellung, wie sich verschiedene europäische Staaten gegen die aufkommende Bedrohung der ausländischen Einflussnahme verteidigen. In dieser Arbeit wird analysiert, wie die Verteidigung von Deutschland, Frankreich, Schweden und Österreich ausgestaltet ist und worin sich die einzelnen Länder unterscheiden. Ebenso wird analysiert, welche Rolle die Europäische Union bei der Konvergenz der unterschiedlichen Strategien und Maßnahmen innehat. Zur Beantwortung dieser Fragen werden die Strategiedokumente der Staaten qualitativ analysiert und miteinander verglichen. Hierbei zeigt sich, dass die vergangenen Erfahrungen der Staaten sowie die Institutionen und Richtlinien der Europäischen Union Einfluss auf die Ausgestaltung der Abwehrmaßnahmen haben. Ebenso zeigt sich, dass die Zusammenarbeit der Staaten im Rahmen der EU zu einer Konvergenz der unterschiedlichen Strategien und zu verstärkter Kooperation führt.

Inhalt

1 Einleitung 5
1.1 Definitionen und Begriffserklärungen 7
1.2 Die Entwicklung von FIMI im Laufe der Zeit 10
1.3 Forschungsfrage und ihre Relevanz 13
1.4 Der Niinistö Bericht 15
2 Internationales Recht und FIMI 16
2.1 Verletzung der staatlichen Souveränität und der Online-Raum 16
2.2 Der Grundsatz der „Non-Intervention“ 17
2.3 Das Prinzip der „Due Diligence“ und das Korfu-Kanal Beispiel 19
2.4 Internationale Menschenrechte 20
2.5 Humanitäres Völkerrecht 22
3 Theoretischer Rahmen - Warum entstehen Policy Änderungen? 23
3.1 Sicherheits-Policy Veränderungen durch Krisen – die „Coordinative Europianisation“. 23
3.2 Policy Änderungen durch Lerneffekte von anderen Staaten – Die „Offene Methode der Koordinierung“ Lesson learning policy drawing. 27
3.3 Historischer Institutionalismus 30
4 Europäischen Maßnahmen, Initiativen und Pläne 32
4.1 Maßnahmen im Rahmen der EU-Außen- und Sicherheitspolitik 33
4.2 HWP ERCHT 36
4.3 Digital Service Act und Digital Markets Act 37
4.4 Die digitale Souveränität der EU 40
5 Sicherheitspolitische und außenpolitische Bedrohungsakteure 41
5.1 Russland als Bedrohungsakteur 42
5.2 China als Bedrohungsakteur 46
6 Die Strategien zur Abwehr von FIMI-Kampagnen 49
6.1 Die DISARM-Methode 49
6.2 Inhaltsmoderation und Entfernen von FIMI-Vorfällen 51
6.3 Fact-Checking, Strategische Kommunikation und Korrektursysteme 53
6.4 Präventive Strategien, Medienlandschaften und „Digital Literacy“ 54
6.5 Die Attribuierung der Urheber und Sanktionen gegen Staaten 57
7 Methodisches Vorgehen 57
7.1 Verwendete Methode 58
7.2 Fallauswahl 59
7.3 Limitationen 60
8 Die Fallstudien 61
8.1 Fallstudie: Deutschland – Strategische Anpassung nach Krisen 61
8.1.1 Die Bedrohungslage und Bedrohungsgeschichte 62
8.1.2 Die Nationale Sicherheitsstrategie 63
8.1.3 Die involvierten Stellen und Behörden und bestehende Maßnahmen 64
8.1.4 Conclusio Deutschland 66
8.2 Fallstudie: Frankreich – Policy-Veränderungen aufgrund von Krisen 67
8.2.1 Die Bedrohungslage 67
8.2.2 Die französische nationale Sicherheitsstrategie 69
8.2.3 Die Struktur der FIMI-Abwehr 71

8.2.4 Conclusio Frankreich 72
8.3 Fallstudie: Schweden – Das Konzept der psychologischen Verteidigung 73
8.3.1 Die Bedrohungslage 74
8.3.2 Die Organisation der FIMI-Abwehr 75
8.3.3 Conclusio Schweden 78
8.4 Fallstudie Österreich – Erste Schritte zur FIMI-Verteidigung 78
8.4.1 Die Bedrohungslage 78
8.4.2 Das Konzept der umfassenden und der geistigen Landesverteidigung 80
8.4.3 Die österreichische Sicherheitsstrategie von 2024 82
8.4.4 Die involvierten Behörden und NGOs 83
8.4.5 Conclusio Österreich 84
9 Ergebnisse und Beitrag zur Fachdebatte 85
10 Weitere Entwicklung der europäischen FIMI-Abwehr und geopolitischer Ausblick 87
11 Literaturverzeichnis 92

1 Einleitung

„Unsere Online-Welt ist ein geopolitisches Schlachtfeld geworden."

Mit diesen dramatischen Worten beginnt das Vorwort der EU-Außenbeauftragten Kaja Kallas des jährlichen FIMI-Berichts des Europäischen Externen Dienstes 2025. (EEAS 2025) Diese Worte und der Bericht zeigen deutlich, dass ausländische Beeinflussung durch Desinformation ein Sicherheitsproblem für die EU und die Souveränität der Mitglieder darstellt. Diese Worte zeigen aber auch, dass die Problematik der hybriden Kriegsführung von Seiten der europäischen Spitzenpolitik erkannt worden ist und, dass inzwischen erste Gegenmaßnahmen gesetzt werden und Verteidigungsstrukturen aufgebaut werden. (EEAS 2025) Die ausländische Einflussnahme auf Prozesse, Entscheidungen und politische Diskurse in anderen Staaten ist kein neues Phänomen. Allerdings hat die Beeinflussung westlicher Staaten durch Russland und andere internationale Akteure in den letzten Jahren eine Intensität erreicht, die eine ernsthafte Gefahr für den öffentlichen Meinungsaustausch, einen Grundpfeiler der liberalen Demokratie, darstellt. (Lahmann 2020)

Insbesondere im so genannten „Superwahljahr 2024" versuchten verschiedene staatliche oder staatsnahe ausländische Akteure durch große und koordinierte Desinformationskampagnen Einfluss auf demokratische Prozesse, politische Diskurse und die öffentliche Meinung, im Sinne wirtschaftlicher oder politischer Interessen, zu nehmen. Ziele dieser Einflussnahmen können sowohl Einzelpersonen als auch einzelne Gruppen und die Gesamtbevölkerung sein. (Berger und Freihse 2024) Für offene Gesellschaften und liberale Demokratien ist es essenziell, dass es Räume gibt, in denen die freie Meinungsbildung und Meinungsäußerung geschehen kann. Da diese Räume allen frei zugänglich sein müssen, können auch Akteure aus dem Ausland mit überwiegend feindseligen Absichten auf diese Räume zugreifen und den Prozess der Meinungsbildung durch Desinformation und Manipulation zu ihren Gunsten beeinflussen. Somit wird das Vertrauen in die liberale Demokratie und in staatliche Institutionen untergraben, radikale politische Positionen gefördert und eine Spaltung der Gesellschaft herbeigeführt. (Bridgman u. a. 2024, 5–6) Des Weiteren finden FIMI-Kampagnen nicht isoliert statt, sondern sind in dem breiteren Kontext der hybriden Kriegsführung zu betrachten. Bei der hybriden Kriegsführung versucht man einen anderen Staat durch nicht konventionelle

Mittel, wie Cyberangriffe, Desinformation oder wirtschaftlichen Druck, zu destabilisieren, ohne einen offenen Krieg zu führen. (Bleyer-Simon 2025)

Immer mehr Staaten nutzen Desinformation und FIMI, um die Bürger anderer Staaten und deren Meinungen zu beeinflussen. Bradshaw und Howard (2020) schreiben, dass im Jahr 2020 bereits mindestens sieben Staaten solche Kampagnen unterhalten. Zu diesen Ländern zählen Russland, China, Indien, Pakistan, Iran, Saudi-Arabien und Venezuela. Da Staaten, insbesondere autokratische Staaten, voneinander lernen, kann man davon ausgehen, dass inzwischen weitere Staaten solche Kampagnen betreiben. (Bradshaw und Howard 2020)

Gegenstand dieser Masterarbeit sind die Strategien und Policy-Ansätze europäischer Staaten zur Bekämpfung ausländischer Desinformationskampagnen, im Englischen als ‚Foreign Information Manipulation and Interference' (FIMI) bezeichnet. Zur Beantwortung der Forschungsfrage werden Fallstudien von vier verschiedenen europäischen Staaten, die eigene „FIMI-Policies" und Abwehrstrategien eingeführt haben, erstellt und anschließend miteinander verglichen. Der Fokus liegt hierbei darauf, herauszufinden aufgrund welcher Faktoren sich die „Policies" in den ausgewählten Staaten unterscheiden und wie sich die jeweiligen Wege und Pfade zu den Verteidigungsstrategien unterscheiden. Ebenso werden die Gründe untersucht, die zu einer Konvergenz und Harmonisierung der Strategien der verschiedenen Länder führen. In der bestehenden Literatur steht zumeist der angreifende FIMI-Akteur sowie dessen Beweggründe, Vorgehen und verwendete Methoden im Vordergrund. Zur Fragestellung, wie sich Staaten verteidigen und wie sich Verteidigungsstrategien entwickeln, gibt es bislang noch vergleichsweise wenig Forschung.

Zu Beginn der Arbeit wird erklärt um welche Art von Bedrohung es sich bei FIMI handelt und aus welchen Gründen Gefahren für souveräne Staaten und demokratische Systeme bestehen. Anschließend wird erläutert, wie FIMI im Rahmen des internationalen Rechts zu betrachten ist und welche internationalen Rechtsnormen und Verträge zur Anwendung kommen können. Im dritten Kapitel werden die gängigen Theorien erläutert, warum sich bestehende Policies in Ländern ändern beziehungsweise angleichen und welche Auslöser diese Veränderungen herbeiführen. Anschließend werden im vierten Kapitel die beiden großen internationalen Bedrohungsakteure, Russland und China, sowie deren Vorgehensweisen, Strategien und Ziele

beschrieben und analysiert. Wenn man versteht, wie der Angreifer vorgeht und welche Ziele dieser verfolgt, kann auch nachvollzogen werden, wie man sich effektiv verteidigen kann. In den folgenden beiden Kapiteln wird zunächst die angewandte Methodik beschrieben und dann die einzelnen Fallstudien zu den ausgewählten Ländern näher betrachtet. Abschließend werden die Ergebnisse der Fallstudien zusammengefasst und miteinander verglichen. Diese Ergebnisse werden zudem in Zusammenhang mit der Fachliteratur gesetzt, um die Entwicklungen der FIMI-Abwehr mit den gängigen Theorien zu Policy-Veränderungen zu erklären. Im letzten Kapitel werden die europäischen Bemühungen in den Kontext der sich stetig verändernden geopolitischen Weltlage gebracht.

1.1 Definitionen und Begriffserklärungen

Seit dem ersten medienwirksamen Bekanntwerden von internationalen Beeinflussungsversuchen im Rahmen der US-Präsidentschaftswahlen 2016 durch Russland hat sich das akademische, politische und journalistische Interesse für das Thema massiv gesteigert. Dadurch ist auch eine Vielzahl von Begriffen und Definitionen geschaffen worden, die meist eine ähnliche Bedeutung haben. Häufig verwendete Formulierungen sind: „Desinformation“, „Fake News“, „Information Operations“ oder „cognitive Warfare“. (Lahmann 2020) Der „European External Action Service“ (EEAS) hat für ausländische Desinformationskampagnen den Begriff FIMI geschaffen. Dieser ist ein Akronym für „Foreign Information Manipulation and Interference“. (EEAS 2024b) Dabei beschreibt der EEAS das FIMI-Phänomen wie folgt:

“Foreign Information Manipulation and Interference (FIMI) describes a mostly non-illegal pattern of behaviour that threatens or has the potential to negatively impact values, procedures, and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner. Actors of such activity can be state or non-state actors, including their proxies inside and outside of their own territory.” (EEAS 2023)

In der wissenschaftlichen Debatte gibt es allerdings auch Kritik an dieser Definition. Der Autor Ofer Fridman (2024) schreibt etwa, dass internationale Einflussnahmen und Beeinflussung ein traditioneller Bestandteil der Außenbeziehungen und der Diplomatie von Staaten seien. FIMI sei daher nur dann ein Problem, wenn erstens die Einflussnahme im Geheimen oder verdeckt

geschieht und wenn zweitens FIMI vom beeinflussten Staat als widersprüchlich zu den eigenen Werten, Normen und Gesetzen wahrgenommen wird. (Fridman 2024) Ausländische Beeinflussung und Manipulation, die von einer Regierung gewünscht wäre, würde daher laut Fridmans Definition nicht als FIMI definiert werden. Als Verbesserung für die Definition des EEAS bietet Fridman daher folgende alternative Definition an:

„*Foreign influence can be characterized as foreign interference when the deployment of different sources of national power (diplomatic, information, military, economic, financial, religious, etc.) by one international actor to influence another is perceived by the latter as in contradiction with his values, norms, or laws*" (Fridman 2024, 12)

Diese Masterarbeit befasst sich mit europäischen Staaten, die mit dem EEAS zusammenarbeiten, an der Erstellung von dessen Berichten mitwirken und sich an dessen Initiativen beteiligen. Daher wird in dieser Arbeit der Definition des EEAS der Vorzug gegeben.

Der Begriff Desinformation sollte darüber hinaus nicht mit den beiden verwandten Begriffen „Malinformation" und „Fehlinformation" verwechselt werden. Bei „Malinformation" handelt es sich grundsätzlich um wahre Informationen. Diese können zum Beispiel persönliche, vertrauliche oder geheime Informationen sein, die veröffentlicht und verbreitet werden, um durch die Veröffentlichung Schaden zu verursachen. Ebenso handelt es sich um Malinformation, wenn ursprünglich wahre Information in einer verfälschten Weise dargestellt wird, sodass durch diese Darstellung Schaden verursacht wird. (Wardle und Derakhshan 2017, 20–22) Ein prominentes Beispiel für Malinformation der jüngeren Geschichte ist die Veröffentlichung gestohlener Emails des „Democratic National Committee" und von John Podesta, dem Wahlkampfmanager von Hillary Clinton, während des US-Präsidentschaftswahlkampfs 2016 durch die Aufdecker-Gruppe Wikileaks. Hackergruppen, die dem russischen Geheimdienst GRU nahestehen, haben sich mittels Phishing-Angriffen Zugriff zu verschiedenen E-Mail-Konten der Demokraten verschafft und deren Inhalte an Wikileaks weitergegeben. Wikileaks hat diese Dokument anschließend veröffentlicht. Diese Veröffentlichungen haben mutmaßlich das Wahlergebnis zu Gunsten von Donald Trump beeinflusst. (Galante und Ee 2018) Bei „Fehlinformation" oder „Misinformation" handelt es sich wiederum um unwahre beziehungsweise falsche Informationen, die ohne die Absicht der

böswilligen Manipulation verbreitet werden. Es besteht also keine Absicht, durch die Veröffentlichung dieser falschen Informationen Schaden zu verursachen. (Wardle und Derakhshan 2017, 20–22) Dies kann zum Beispiel etablierten Medienunternehmen durch Unachtsamkeit oder durch mangelnde journalistische Sorgfalt passieren.

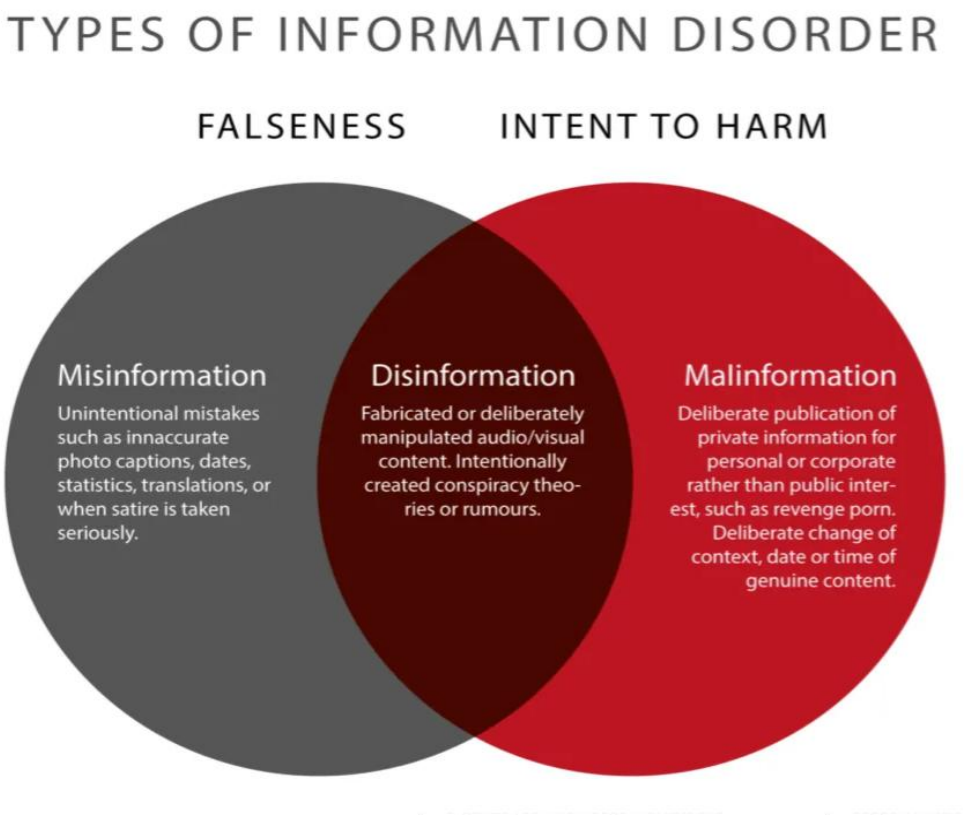

Abbildung 1: Wardle und Derakshan (2017)

In diesem Zusammenhang müssen auch mögliche Überschneidungen der beiden Begriffe bedacht werden. Durch die Möglichkeiten des Teilens sowie des Weiterleitens von Inhalten auf sozialen Medien können Nutzende ungewollt dazu beitragen, dass aus Desinformation Fehlinformation wird. Sollten Nutzenden Informationen, die Desinformation beinhalten, weiterverteilen, entsteht dadurch Fehlinformation, weil die bewusste Verbreitung von Unwahrheiten sowie die Absicht der Manipulation nicht mehr länger gegeben ist. (Humprecht u. a. 2020, 5)

Wenn man über den Begriff FIMI spricht, stellt sich des Weiteren die Frage, an welchem Punkt legitimer ausländischer Einfluss, der zum Beispiel durch die diplomatischen Beziehungen zwischen zwei Ländern ausgeübt wird, endet und an welchem Punkt illegale und illegitime

Einmischung beziehungsweise Beeinflussung beginnt. Zwischen diesen beiden Polen existiert auch eine Grauzone, in der sich ausländische Einflussnahmen befindet, die zwar den Werten eines Landes widersprechen, aber nicht dezidiert illegal sind. (Mansted 2021) Es spricht grundsätzlich wenig dagegen, wenn ein Staat in einem anderen Staat eine Tourismuskampagne betreibt und dabei die Qualitäten des eigenen Landes überzeichnet darstellt. Maßnahmen zur FIMI-Abwehr müssen daher auch vor dem Hintergrund dieser legitimen Einflussnahmen und Grauzonen gedacht werden. Es ist nicht der Sinn von FIMI-Abwehrmaßnahmen, diplomatische Beziehungen zu sabotieren, jeglichen ausländischen Einfluss zu beenden und ein Land vollständig zu isolieren. (Fridman und Boucher 2024)

1.2 Die Entwicklung von FIMI im Laufe der Zeit

Ausländische Desinformationskampagnen sind an sich keine neue Erfindung, auch wenn der Begriff FIMI als solcher ein neuer ist. (Chłoń u. a. 2024) Zum Beispiel haben die Alliierten während des Zweiten Weltkriegs, im Rahmen der Operation „Bodyguard“, mittels falscher Funksprüche und Militärberichte die Erzählung verbreitet, dass eine Alliierte Invasion in der Nähe von Calais stattfinden wird und nicht in der Normandie. Die NS-Führung konnte mit dieser Operation getäuscht werden und die Landung in der Normandie erfolgreich durchgeführt werden. (Schulze 2019)

Im Jahr 2016 sind sowohl die breite Öffentlichkeit als auch die wissenschaftliche Gemeinschaft zuerst durch den Erfolg des BREXIT-Referendums und anschließend durch den Sieg von Donald Trump bei den US-Präsidentschaftswahlen darauf aufmerksam geworden, wie effektiv Desinformationen auf sozialen Medien sein können und wie divers die Einsatzmöglichkeiten sind. (Persily und Tucker 2020, 21–23) Insbesondere die russische Einflussnahme auf die US-Präsidentschaftswahl 2016 gilt als ein Paradebeispiel für FIMI. Allerdings lässt sich russische Einflussnahme bereits im Jahr 2014 im Rahmen der Besetzung der Krim-Halbinsel beobachten. (Fridman 2024) Auch wenn internationale Desinformation schon lange besteht, ist FIMI in seiner heutigen fortgeschrittenen Form und hohen Intensität allerdings ein neues Phänomen, dass insbesondere durch den völkerrechtswidrigen russischen Angriffskrieg in der Ukraine an Bedeutung gewonnen hat. Auch die Entwicklung moderner Technologien sowie die rasante Verbreitung des Internets und der sozialen Medien führen dazu, dass man mit FIMI immer

mehr Menschen immer leichter und kostengünstiger erreichen und manipulieren kann. (EEAS 2023, 7) FIMI ist das neueste Werkzeug von Staaten in der internationalen Politik. Es wird von manchen Staaten wesentlich häufiger eingesetzt als von anderen. Im Kern ist es allerdings nur ein weiteres strategisches Werkzeug zur Durchsetzung nationalstaatlicher Interessen auf der globalpolitischen Ebene. (Chłoń u. a. 2024, 2)

Phillip Howard (2020) beschreibt die FIMI-Maschinerien von Staaten, politischen Organisation und großen Unternehmen als „Lie Machines“. Bei diesen handelt es sich um Personen, Gruppen und Organisationen, die moderne Technologien und die Verfügbarkeit von großen Datenmengen dazu nutzen, falsche Nachrichten zu erstellen und zu verbreiten. Ziel dieses Vorgehens ist es, politische Ziele und strategische Interessen durchzusetzen. Als bekanntes Beispiel hierfür führt er die Aktionen von chinesischen Aktivisten an, die im Rahmen der Hong Kong Proteste im Jahr 2019 mittels falscher Nachrichten versucht haben, den Rest der Welt davon zu überzeugen, dass es sich bei den Protestierenden um eine kleine, radikale und gewaltvolle Splittergruppe handelt, die über keine Unterstützung in der breiten Zivilgesellschaft verfügt. (Howard 2020) Im digitalen Zeitalter haben sich die Werkzeuge, mit denen Desinformation verbreitet wird verändert. Inzwischen finden Desinformationskampagnen überwiegend im digitalen Raum statt. Hier wird Desinformation insbesondere über Soziale Medien und Messenger Dienste wie „Telegram“ verbreitet. Mit diesen kann man eine Vielzahl an manipulierten Nachrichten ortsunabhängig und innerhalb kürzester Zeit an ein potenzielles Millionenpublikum verbreiten. (Bradshaw und Howard 2020) Soziale Medien sind auch deshalb für ausländische Akteure interessant, weil sie dort kaum oder nur unzureichend moderiert werden, sich Nachrichten besonders schnell verbreiten und immer mehr Menschen soziale Medien zur politischen Informationsbeschaffung nutzen (Humprecht u. a. 2020) Einen weiteren Vorteil, den soziale Medien für die Verbreitung von Desinformation bieten, ist die Möglichkeit zielgerichtet bestimmt thematische Nischen zu bedienen, die für bestimmte Botschaften besonders Empfänglich sind. Um diese Nischen zu identifizieren, werden Algorithmen verwendet, mit deren Hilfe große Mengen an zum Teil sehr persönlichen Daten ausgewertet werden. (Chłoń u. a. 2024, 3–4) Der 2018 bekannt gewordenen Cambridge-Analytica Skandal hat der Weltöffentlichkeit demonstriert, wie präzise Algorithmen spezifische Nischen und Personengruppen identifizieren können.

(Meredith 2018) Klassische und unabhängige Medien eignen sich für diese Art der Desinformation weniger, da dort in der Regel eine Moderation durch den Eigentümer oder die Redaktion stattfindet. Des Weiteren haften klassische Medien in der Regel für die Inhalte, die sie veröffentlichen. Soziale Medienunternehmen hingegen haften in der Regel nicht für die Inhalte, die von Plattformnutzern auf ihren jeweiligen Plattformen veröffentlicht werden. (Vargo u. a. 2018) Staaten oder deren nicht-staatliche Verbündete, so genannte „Proxies“, können allerdings die Eigentümer klassischer Medienunternehmen sein und diese dann für FIMI verwenden. So ist zum Beispiel bekannt, dass die russischen Medien Sputnik und RT, für FIMI genutzt werden. (EEAS 2025)

In Zukunft werden ausländische Desinformationskampagnen in ihrer Wirkung wahrscheinlich noch potenter. Mit Werkzeugen wie generativer Künstlicher Intelligenz lassen sich falsche Informationen noch überzeugender darstellen und noch mehr Menschen noch besser täuschen. (Schulze 2019) Zum Schutz demokratischer Prozesse, der Souveränität von Staaten und ihrer „raison d’etre“ ist es wichtig, dass die Bevölkerung der Staaten sowie die Staaten selbst Resilienzen gegen Desinformation aufbauen und, dass die Staaten Strategien und Maßnahmen einführen, mit denen man sich gegen diese Art der hybriden Kriegsführung verteidigen kann. (Dowling 2021)

Demokratische und liberale Länder stehen hierbei vor einer besonderen Herausforderung. Sie müssen stets zwischen dem Blockieren beziehungsweise dem Entfernen von illegitimer Desinformation und der Wahrung der Meinungsfreiheit abwägen. Durch das Blockieren und Entfernen von Inhalten ergibt sich stets auch die Gefahr der staatlichen Zensur. Das absichtliche oder unabsichtliche Unterdrücken und Entfernen von legitimer Information unter dem Vorwand, es handle sich um Desinformation, kann schwerwiegende Auswirkungen auf die freie Meinungsbildung haben. (D’Andrea u. a. 2025) Menschen benötigen, zur Ausübung ihrer demokratischen Mitbestimmungsrechte sowie ihrer Grund- und Freiheitsrechte, uneingeschränkten Zugriff auf faktisch richtige Informationen. Ebenso werden diese Informationen benötigt, um die tagtäglichen Bedürfnisse zufrieden zu stellen. (Chłoń u. a. 2024)

1.3 Forschungsfrage und ihre Relevanz

In dieser Masterarbeiter wird folgender Forschungsfrage nachgegangen: Welche Strategien und Policy-Maßnahmen implementieren ausgewählte europäische Länder zur Abwehr und Bekämpfung von FIMI-Kampagnen? Welche relevanten Unterschiede gibt es zwischen den verschiedenen Ländern und wie kann man eine mögliche Konvergenz der Strategien im Laufe der Zeit erklären? Es ist auch ein Ziel dieser Arbeit, Handlungsempfehlungen für Staaten abzuleiten, beziehungsweise „Best-Practice" Beispiele aufzuzeigen.

Die bestehende Literatur widmet sich zumeist der Analyse der Angreifer sowie ihrer Methoden, wohingegen den Verteidigungsmöglichkeiten und -Strategien von betroffenen Staaten nur wenig Aufmerksamkeit gewidmet wird. Insbesondere ist es bislang unbekannt, aus welchen Gründen es große Unterschiede zwischen den Verteidigungs-policies europäischer Staaten gibt, obwohl diese in vielen Bereichen eng miteinander zusammenarbeiten und man daher annehmen könnte, dass große Ähnlichkeiten zwischen den Strategien der unterschiedlichen Staaten bestehen. Zurzeit ist FIMI für die europäischen Staaten noch ein relativ neues Phänomen, daher ist es möglich, dass unterschiedliche Staaten in ihrer anfänglichen Reaktion unterschiedliche Strategien und Maßnahmen einführen, diese aber im Lauf der Zeit immer mehr vereinheitlichen. Im Rahmen diverser EU-Koordinierungsgremien können die Staaten voneinander und miteinander lernen und ihre Vorgehensweisen immer mehr angleichen.

Wie eingangs erwähnt, stellen Desinformation und ausländische Beeinflussung inzwischen ein ernsthaftes Risiko für die staatliche Souveränität dar, weil ausländische Akteure durch die gezielte Verbreitung von Desinformation erheblichen Einfluss auf die demokratischen und politischen Prozesse eines Landes nehmen können. (Dias 2023) Des Weiteren stellt auch die Reaktion auf FIMI-Bedrohungen ein Risiko für die Grundrechte und die demokratischen Prozesse dar. Durch zu ausufernde Maßnahmen können sowohl die Meinungs- und Redefreiheit als auch die Möglichkeit der demokratischen Teilnahme eingeschränkt werden. (Veiga 2025) Vor dem Hintergrund dieser Risiken sowie den rasant fortschreitenden technologischen Entwicklungen, die sowohl die Reichweite als auch die Wirksamkeit von FIMI-Kampagnen noch weiter erhöhen, ist es von entscheidender Bedeutung zu eruieren, wie die

derzeitigen Verteidigungs-Policies beschaffen sind und welche Policy-Maßnahmen es in diesem Bereich gibt. Eine frühzeitige Vorbereitung gegen FIMI-Kampagnen sowie eine rasche Reaktion auf bekannt gewordende FIMI-Kampagnen sind entscheidend zur erfolgreichen Verteidigung. FIMI-Kampagnen bieten aufgrund ihrer Eigenschaften viele Vorteile für den Angreifer und machen dadurch eine erfolgreiche Abwehr für den Verteidiger schwierig. Diese Vorteile sind: Erstens verursachen FIMI-Kampagnen für die Angreifer in der Regel nur geringe Kosten. Damit einher geht ein geringes Risiko, während die potenziellen Gewinne im Falle eines Erfolges sehr hoch sind. Da FIMI-Angriffe im Rahmen der hybriden Kriegsführung oft verdeckt erfolgen, ist zudem eine klare und eindeutige Attribuierung der Angreifer für den Verteidiger schwierig. Der Angreifer kann sich stets auf die „plausible deniability" berufen, mit der er jede Verantwortung von sich weisen kann. Dadurch ist es für den Zweitens verfügen die Angreifer über den so genannten „First mover advantage", der besagt, dass derjenige, der zuerst aktiv ist und die Initiative innehat, einen Vorteil gegenüber dem Reagierenden hat. Eine FIMI-Kampagne kann bereits vollständig aktiv sein, bevor sie von den Behörden aufgedeckt wird und dem entsprechend Gegenmaßnahmen ergriffen werden können. Durch diesen Vorteil sind die Behörden und die nationalen Regierunngen stets darauf beschränkt zu reagieren und sind nicht in der Lage, selbst die Initiative zu ergreifen. Drittens sind die Angreifer nicht durch bürokratische, legale und ethische Hürden und Bedenken eingeschränkt, die rechtsstaatlich agierende Behörden hingegen bei ihren Verteidigungsmaßnahmen gegen FIMI-Kampagnen stets berücksichtigen müssen. Viertens sind auch die Reaktionen der europäischen Staaten für die Angreifer von Vorteil. So gibt es in manchen Staaten nach wie vor keinen ausreichenden politischen Willen, FIMI-Vorfälle als solche anzuerkennen, eine Attribuierung vorzunehmen sowie die Täter zu bestrafen. In manchen Fällen profitieren europäische Politiker und Parteien sogar von ausländischer Einflussnahme, weil mit ihnen diese Kampagnen zu politischem Erfolg verhelfen. (Pamment 2020b)

Vor dem Hintergrund dieser vielen Vorteile für den Angreifenden ist es umso wichtiger, dass Staaten sich mittels eigener FIMI-Policies und Abwehrstrategien vorbereiten und, dass bereits frühzeitig mit dem Aufbau von gesellschaftlicher Resilienz begonnen wird. Aus diesem Grund widmet sich diese Masterarbeit der Fragestellung, aus welchen Gründen sich die FIMI-Abwehr Policies verschiedener Länder unterscheiden und wie europäische Kooperations- und

Koordinierungsmechanismen zu einer verstärkten Konvergenz verschiedener Strategien führen.

1.4 Der Niinistö Bericht

Im Oktober 2024 wurde von dem ehemaligen finnischen Präsidenten Sauli Niinistö, in seiner Funktion als „Special Advisor“ für die Europäische Kommission, ein Bericht mit dem Titel „Safer Together - Strengthening Europe’s Civilian and Military Preparedness and Readiness“ veröffentlicht. In diesem Bericht, der inzwischen als der „Niinistö Bericht“ bekannt geworden ist, wird dargelegt, dass die EU ihre gemeinsame Sicherheitspolitik vereinheitlichen sollte und, dass die militärische Resilienz und die zivile Resilienz der Mitgliedstaaten, insbesondere gegenüber hybriden Bedrohungen, gestärkt werden sollte. (Niinistö 2024) In diesem Bericht wird der EU und den Mitgliedern nahegelegt, sich basierend auf dem finnischen Modell der „all-hazards and all-risks“, vorzubereiten. Gefordert wird, dass man gegen zivile, klimatische, wirtschaftliche und militärische Bedrohungen bestehen kann. Ein Kerngedanke des „all hazards all risks“ Ansatzes ist, dass sich nicht nur Regierungen und die öffentliche Verwaltung mit der Krisen- und Gefahrenvorbereitung befassen, sondern auch Unternehmen, Privatpersonen und die Zivilgesellschaft. Es handelt sich also um einen gesamtgesellschaftlichen Ansatz. (Iso-Markku und Helwig 2024)

Die Staaten Europas sind aufgrund ihrer offenen, demokratischen Gesellschaften und der weitgehend herrschenden Meinungsfreiheit besonders verwundbar gegenüber FIMI-Kampagnen. Solche Kampagnen sind für Akteure wie China oder Russland sehr günstig durchzuführen, bringen ihnen aber gleichzeitig großen Nutzen, indem dadurch die Einigkeit zwischen den Mitgliedsstaaten und die Harmonie und der Zusammenhalt innerhalb der Mitgliedstaaten geschwächt wird. Die europäische Union und ihre Mitglieder befinden sich in einem systemischen Wettbewerb mit anderen globalen Großmächten und diese nutzen die Schwächen der demokratischen Gesellschaften aus. Eine EU, die uneinig auftritt und mit sich selbst beschäftigt ist, ist für andere Großmächte leichter zu kontrollieren und für deren geopolitischen Entscheidungen weniger relevant. (Niinistö 2024, 42) Speziell im Kapitel zur Bedrohung durch FIMI schreibt Niinistö (2024), dass es zur Stärkung der Resilienz vermehrter politischer Bildung sowie vermehrter Demokratiebildung bedarf und, dass man, insbesondere

vor dem Hintergrund der Entwicklungen im Bereich der Künstlichen Intelligenz, die „Media-Literacy“ der Bürger stärken müsse. Wenn man die Resilienz der Bürger in diesen Bereichen stärkt, reduziert man die Kosten-Effizient von FIMI-Angriffen, wodurch solche Angriffe für die Angreifer weniger interessant werden. (Niinistö 2024, 74–75) Des Weiteren empfiehlt der Niinistö Bericht, dass die EU-Mitglieder verstärkt zusammenarbeiten und ein gemeinsames Konzept zur Früherkennung von Bedrohungen ausarbeiten. (Niinistö 2024)

2 Internationales Recht und FIMI

Wenn man FIMI-Bedrohungen aus der Sicht des internationalen Rechts betrachtet, muss zuerst festgehalten werden, dass es im internationalen Recht und innerhalb der internationalen Normen keine Regelungen und Verträge gibt, die speziell für FIMI geschaffen worden sind. In den vergangenen Jahren sind einige Vorschläge für neue internationale Rechtsnormen eingebracht worden. Die Staatengemeinschaft konnte sich jedoch bislang nicht auf einen neuen rechtlichen Rahmen einigen. Trotz der Abwesenheit konkreter FIMI bezogener Rechtsnormen können andere Rechtsnormen zur Regulierung und Einordnung vom FIMI herangezogen werden. Hier spielen insbesondere die generellen Prinzipien und Normen im internationalen Recht eine Rolle. (Dias 2023) Der Einsatz von ausländischen Desinformationskampagnen verstößt unter Umständen in mehreren Punkten gegen geltendes internationales Recht oder bestehende internationale Normen. An dieser Stelle muss auch erwähnt werden, dass es verschiedene Arten von FIMI gibt, die sowohl legitim als auch illegitim sein können. Legitime ausländische Beeinflussung kann daher zwar völkerrechtlich legal sein, aber dennoch Schaden verursachen. FIMI auf der anderen Seite kann völkerrechtswidrig sein, ohne Schaden zu verursachen. Diese unterschiedlichen Arten von FIMI sind rechtlich unterschiedlich zu behandeln. (Dias 2023)

2.1 Verletzung der staatlichen Souveränität und der Online-Raum

“All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.” Art. 2(4) UN-Charta

Die staatliche Souveränität ist ein Grundstein der internationalen Ordnung. Sie garantiert, dass Staaten, innerhalb ihrer Grenzen, ihre legislativen, judikativen und administrativen Kompetenzen souverän ausüben können. (Benthem u. a. 2022) Im Sinne der souveränen Gleichheit müssen Staaten die Souveränität anderer Staaten anerkennen. Das bedeutet auch, dass Staaten die exklusive Hoheitsgewalt über die Menschen innerhalb ihres Territoriums verfügen und andere Staaten diese exklusive Hoheitsgewalt respektieren. FIMI-Operationen, die von einem Staat oder staatsnahen Gruppen durchgeführt werden und dabei einen anderen Staat in der Ausübung seiner staatlichen Kompetenzen und, oder seiner staatlichen Aufgaben behindern, verstoßen demnach gegen das Prinzip der staatlichen Souveränität. Eine staatliche Kernaufgabe ist zum Beispiel die Durchführung von demokratischen Wahlen. Verbreitet ein angreifender Staat gezielt Desinformation über die Durchführung demokratischer Wahlen in einem anderen Staat, verletzt er damit das Prinzip der staatlichen Souveränität. Der betroffene Staat kann seine administrativen Hoheitsbefugnisse nicht länger uneingeschränkt ausüben. (Dias 2023)

Es gibt allerdings auch Gegenstimmen wie jene von Ohlin (2020), die behaupten, dass das Konzept der Souveränität im Falle einer ausländischen Wahlbeeinflussung nicht angewendet werden kann. Eine Verletzung der staatlichen Souveränität setze voraus, dass entweder die territoriale Integrität verletzt wird oder von einem anderen Staat entweder Zwang oder eine staatliche Funktion ausgeübt wird. FIMI beziehungsweise die Beeinflussung der Wähler und des Wählerwillens ist laut Ohlin dennoch illegal, allerdings nicht aufgrund das Souveränitätsprinzip. Die Beeinflussung des Wählerwillens durch FIMI stellt keine Verletzung staatlicher Souveränität. Ausländische Beeinflussung, insbesondere Wahlbeeinflussung stellt allerdings eine Verletzung des Selbstbestimmungsrechts der Völker dar. (Ohlin 2020)

2.2 Der Grundsatz der „Non-Intervention“

Der Grundsatz der Nicht-Einmischung oder der „Non-Intervention“ in die internen und externen Angelegenheiten eines anderen Staates hängt mit dem Prinzip der staatlichen Souveränität nach Artikel 2 (4) der UU-Charta zusammen. (Dias 2023) In Artikel 2 (7) der UN-Charta ist zur Nicht-Einmischung folgendes festgehalten:

„Nothing contained in the present Charter shall authorize the United Nations to intervene in matters which are essentially within the domestic jurisdiction of any state, or shall require the Members to submit such matters to settlement under the present Charter; but this principle shall not prejudice the application of enforcement measures under Chapter VII." Art. 2 (7) UN-Charta

Der Grundsatz der „Non-Intervention" wird auch als Teil des Volksgewohnheitsrechts betrachtet und gilt somit unabhängig von vertraglichen Regelungen und Bestimmungen und auch für jene Staaten, die die entsprechenden Verträge nicht unterzeichnet beziehungsweise ratifiziert haben. Der Grundsatz der „Non-Intervention" dient dem Schutz kleinerer Staaten vor der Einflussnahme größerer und mächtigerer Staaten. Er gewährleistet, dass kein Staat einem anderen seinen politischen, wirtschaftlichen oder gesellschaftlichen Willen aufzwingen kann. Sollte es erlaubt sein, dass die stärkeren Staaten ihren Willen durchsetzen können, würde dies auch das staatliche Souveränitätsprinzip, welches im Rahmen des Westfälischen Friedens im Jahr 1648 etabliert worden ist, in Frage stellen. (Ohlin 2020) Um das Prinzip der „Non-Intervention zu konkretisieren ist im Jahr 1976 ist von der UN-Generalsversammlung die Resolution 31/91, „Declaration of Non-Interference in the internal Affairs of states", erlassen worden und im Jahr 1980 die Resolution 36/103, „Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States". In diesen beiden Resolutionen wird im Grunde genommen festgehalten, welche Formen der ausländischen Einflussnahme illegal sind. So wird zum Beispiel in der Resolution von 1981 explizit vermerkt, dass diffamierende Kampagnen sowie feindselige Propaganda, die das Ziel haben in die inneren Angelegenheiten von Staaten einzugreifen verboten sind. Des Weiteren schreiben diese Resolutionen den Staaten auch vor, dass sie innerhalb ihrer Territorien gegen die Verbreitung von Desinformation, die als Einmischung in die internen Angelegenheiten anderer Staaten gesehen werden kann, vorgehen müssen. Erstaunlicherweise haben die westlichen Staaten in den Jahren 1976 und 1980 gegen diese Resolutionen gestimmt, da sie befürchtet haben, dass autoritäre Staaten die Resolutionen dazu nutzen könnten, berechtigte Kritik an fehlenden Grund- und Freiheitsrechten als ausländische Einmischung und Verbreitung von Desinformation darzustellen. (Lahmann 2020)

Das Konzept der „Non-Intervention“ deckt allerdings nur staatliche Maßnahmen ab, die durch Zwang den Handlungsspielraum eines anderen Staates einschränken und diesen dazu bringen, Maßnahmen zu unternehmen, die dieser ohne den äußeren Zwang nicht unternommen hätte. Neben dem direkten Zwang, der beispielsweise durch physische Gewalt ausgeübt werden kann, gibt es laut dem Internationalen Gerichtshofe auch den indirekten Zwang, der auch gewisse für FIMI verwendete Vorgehensweisen inkludiert. (Dias 2023, 10) Im Jahr 1986 hat der ICJ hierzu ein wegweisendes Urteil im Verfahren Nicaragua VS United States gefällt. In diesem wird festgehalten, dass auch ausländische Propaganda und Desinformation als Verletzung der „Non-Intervention“ gelten können. (Lahmann 2020) Der Einsatz von Propaganda, Desinformation und Hass-Rede durch Staaten, nicht-staatliche Akteure oder „Proxies“ von Staaten verstößt gegen das Prinzip der“Non-Intervention“, wenn dadurch die Freiheit eines Staats, seine internen und externen Angelegenheiten eigenständig zu regeln, betroffen beziehungsweise eingeschränkt wird. (Dias 2023, 10–11) Diese Ansicht wird auch vom Autoren Steven Wheatley (2019) geteilt, der schreibt, dass Desinformations-Operationen, die darauf ausgelegt sind, die Wählerschaft eines anderen Landes zu einer anderen Wahlentscheidung zu bewegen oder, die darauf abzielen eine Blockade der politischen Handlungsfähigkeit zu erreichen, inhärent zwanghaft sind. Daher sind solche Desinformationskampagnen im Sinne des „Non-Intervention“ Prinzips illegal. Durch die Manipulation der verfügbaren Information wird dem Opfer von FIMI die Freiheit genommen, für sich selbst die richtige Entscheidung zu treffen. (Wheatley 2020) Laut Lahmann (2020) hingegen sind Beeinflussungsversuche kein Verstoß gegen das Prinzip der Non-Intervention, wenn diese offen sind und nicht- geheim sind. Medien wie Sputnik oder RT, die erwiesen russische Propaganda verbreiten, üben durch ihre Offenheit keinen Zwang aus und verstoßen somit nicht gegen die Non-Intervention. Dadurch, dass die Identität des Senders bekannt ist, kann der Empfänger selbst über die Vertrauenswürdigkeit der Quelle entscheiden. (Lahmann 2020)

2.3 Das Prinzip der „Due Diligence“ und das Korfu-Kanal Beispiel

„Due Diligence“ ist eine internationale Rechtsnorm, die besagt, dass Staaten sich so zu verhalten haben, dass Schäden an anderen Staaten nach Möglichkeit vermieden werden. Bei „Due Diligence“ Verpflichtungen geht es in der Regel nicht darum, dass Staaten den Schaden erfolgreich verhindern, sondern, dass sie Versuche unternehmen, um einen drohenden

Schaden zu verhindern. Damit ein Staat für einen entstandenen Schaden verantwortlich gemacht werden kann, muss dieser vorhersehen können, dass ein Schaden entstehen könnte, und es muss innerhalb der Möglichkeiten des Staates liegen, das Eintreten des Schadensfalls zu verhindern. Da Staaten über unterschiedliche wirtschaftliche, gesellschaftliche und politische Möglichkeiten verfügen, um einen Schaden abzuwenden, gelten für unterschiedliche Staaten unterschiedliche Standards. Des Weiteren gibt es bei der „Due Diligence“ die Debatte, ob es sich um ein allgemeines völkerrechtliches Prinzip handelt, welches auf alle Bereiche staatlichen Handelns anwendbar ist, oder ob es sicher hierbei nur um eine Rechtsnorm handelt, die in bestimmten vordefinierten Rechtsbereichen Anwendung findet, wie zum Beispiel im Rahmen des UN-Seerechtübereinkommens. Weil es bislang kein Übereinkommen über das Verhalten von Staaten im Online-Raum gibt, wird von einigen Staaten das Argument vorgebracht, dass Staaten nicht dazu verpflichtet sind, dafür zu sorgen, dass Handlungen die von ihrem Staatsgebiet ausgehen und im Online-Raum stattfinden keine Schäden in anderen Staaten verursachen. (Dias 2023, 11)

Im Bereich der Due Diligence ist der „Corfu-Channel Fall“ zwischen dem Vereinigten Königreich und der Republik Albanien ein häufig genannter Präzedenzfall. In diesem Fall hat der Internationale Gerichtshof festgestellt, dass Staaten, die wissen oder wissen müssten, dass ihr Territorium für Handlungen genutzt wird, die den Rechten eines anderen Staates schaden, verpflichtet sind, diese Handlungen zu unterbinden. Im konkreten Fall hätte die Republik Albanien verhindern müssen, dass britische Schiffe durch Seeminen, von denen Albanien behauptet, sie seien von Griechen während des Griechischen Bürgerkriegs ausgelegt worden, im Korfu-Kanal beschädigt werden, wobei zahlreiche Menschen ums Leben gekommen sind. Im Bereich der FIMI bedeutet das, dass Staaten gegen die Norm der „Due Diligence“ verstoßen, wenn wissentlich keine Schritte unternommen werden, um andere Staaten oder nicht-staatliche Akteure, die das Territorium des betroffenen Staates nutzen, an der Schädigung eines dritten Staates zu hindern. (Dias 2023, 11)

2.4 Internationale Menschenrechte

Staaten sind durch verschiedene Verträge, Abkommen und Normen, wie zum Beispiel die Europäische Menschenrechtskonvention oder die Allgemeine Erklärung der Menschenrechte,

an Menschenrechte gebunden. Diese Menschenrechte haben auch im Online-Raum ihre Gültigkeit. (Dias 2023, 12–13) Daher stellt sich bei der rechtlichen Einordnung von FIMI auch die Frage, gegen welche Menschenrechte Staaten beim Einsatz von FIMI verstoßen können und welche Rolle die Aufrechterhaltung der Menschenrechte beim Vorgehen gegen FIMI-Kampagnen spielt. Des Weiteren ergeben sich aus den internationale Menschrechtsnormen Schutzpflichten des Staates gegenüber Dritten. Das heißt, dass Staaten nicht nur selbst keine Menschenrechtsverletzungen durch FIMI-Kampagnen begehen dürfen, sondern dass sie dafür Sorge tragen müssen, dass ihre eigene Bevölkerung vor den FIMI-Bemühungen anderer Staaten geschützt ist. (UN. Human Rights Committee 2004)

FIMI-Kampagnen greifen häufig auf Hassrede, diskriminierende sowie rassistische Sprache oder Aufrufen zur Gewalt zurück. So kann die Durchführung von FIMI-Kampagnen ein Verstoß gegen Artikel 20 des Internationalen Paktes über die politischen und bürgerlichen Rechte (IPBPR) sein, wenn damit Kriegspropaganda verbreitet oder zur Gewalt aufgerufen wird. Darüber hinaus verbietet Artikel 20 des IPBPR Hass und Kriegspropaganda. Ebenso kann man durch das Betreiben von FIMI-Kampagnen auch gegen das in Artikel 26 IPBPR festgelegte Diskriminierungsverbot verstoßen, wenn FIMI-Kampagnen dazu genutzt, rassistische geprägte und diskriminierende Stereotype zu verbreiten. (Dias 2023, 13)

Insgesamt ergibt sich im Kontext der Menschenrechte und FIMI ein zentrales Spannungsfeld. Staaten haben ein verständliches Interesse an der Bekämpfung und Unterbindung von Desinformation, müssen aber gleichzeitig selbst das Menschenrecht auf frei Meinungsäußerung sowie jenes auf freie und faire Wahlen aufrechterhalten und sicherstellen. Das Recht auf freie Meinungsäußerung ist unter anderem in Artikel 19 des IPBPR und das Recht auf freie und faire Wahlen in Artikel 25 festgehalten. (Dias 2023, 13–14) FIMI-Kampagnen stellen eine Bedrohung für diese demokratischen Selbstbestimmungsrechte dar, indem sie den öffentlichen Diskurs untergraben und Mistrauen in demokratische Institutionen schüren. (Wheatley 2020) Zeitgleich können Maßnahmen, die zur Bekämpfung von FIMI eingeführt werden, auch das Recht auf freie Meinungsäußerung verletzen, indem Behörden die Verbreitung legitimer Informationen unterbinden. Für Staaten ist es schwer die Grenze zwischen legitimer Informationskotrolle und unrechtmäßiger Zensur zu ziehen. Insbesondere autoritär geführte Staaten haben in der Vergangenheit die Erzählung der ausländischen

Beeinflussung genutzt, um oppositionelle sowie unliebsame Meinungen zu unterdrücken. Ein UN-Report aus dem Jahr 2019 empfiehlt daher Staaten nur in Ausnahmefällen einzugreifen und hierfür transparente Kriterien festzulegen. (Kaye u. a. 2019, 6–8) Trotz dieser Vorgaben erlauben internationale Menschenrechtsabkommen Staaten auch eine Einschränkung des Rechts auf freie Meinungsäußerung. So erlaubt beispielsweise der IPBPR in Artikel 19 Absatz 3 den Staaten eine Einschränkung der Meinungsfreiheit, wenn dadurch die Würde und die Rechte anderer gewahrt werden oder wenn es notwendig ist, um die öffentliche Ordnung aufrecht zu erhalten. (Dias 2023, 14) Zur Lösung dieses Spannungsfeldes bekennt sich die EU dazu, dass ihre Strategien im Umgang mit FIMI stets im Einklang mit der Europäischen Menschenrechtskonvention stehen muss. (EEAS 2023)

2.5 Humanitäres Völkerrecht

Humanitäres Völkerrecht gilt für gewöhnlich in internationalen sowie nationalen bewaffneten Konflikten und soll sicherstellen, dass nicht-Kombattanten vor Schädigungen geschützt werden und, dass Kombattanten auf dem Schlachtfeld vor unnötigem Leiden bewahrt werden. Obwohl sich das humanitäre Völkerrecht zumeist auf die traditionellen und militärischen Aspekte der Kriegsführung fokussiert, wie zum Beispiel den Umgang mit Kriegsgefangenen, kann es auch bei Konflikten im Online-Raum und bei FIMI-Operationen Anwendung findet. (Dias 2023, 14) Das Internationale Rote Kreuz hat dazu festgehalten, dass humanitäres Völkerrecht auch im Online-Raum anwendbar ist. Insbesondere sind direkte FIMI-Angriffe auf Zivilisten verboten und bei FIMI-Angriffen gegen Kombattanten müssen die völkerrechtlichen Grundsätze der Proportionalität folgen. (ICRC 2019) Diese Ansicht wird allerdings von einigen Staaten, die die Meinung vertreten zur Regulierung des Online-Raumes brauche es neue internationale Abkommen, verneint. (ICRC 2022) Es ist beispielsweise verboten, FIMI zu Terrorisierung von nicht-Kombattanten einzusetzen oder, um die Arbeit von medizinischem, religiösem oder humanitärem Personal zu verhindern oder zu sabotieren. (Dias 2023, 14) So stellt es beispielsweise ein Verstoß gegen die Artikel 18 und 19 der vierten Genfer Konvention, die den Schutz medizinischer Einrichtungen regeln, dar, wenn mittels einer FIMI-Kampagne die Falschmeldung verbreitet wird, dass ein Krankenhaus für militärische Zwecke genutzt werde, wodurch dieses Krankenhaus ein legitimes militärisches Ziel werden würde und somit angegriffen werden könnte . (ICRC 1949)

3 Theoretischer Rahmen- Warum entstehen Policy Änderungen?

Zur fundierten Beantwortung der Frage: „Warum sich die FIMI-Abwehr Policies und Strategien einzelner Länder unterscheiden?“ muss zunächst verstanden werden, welche Faktoren zu Policy-Veränderungen führen und welche Faktoren ausschlaggebend für unterschiedliche Ausprägungen und Ausgestaltungen sind. In diesem Theoriekapitel wird auf den aktuellen Stand der Forschung eingegangen und einige gängigen theoretischen Ansätze erläutert. Da es sich bei FIMI-Policies um ein dynamisches und mehrschichtiges Feld handelt, das verschiedene Politikbereiche, sich unterscheidende nationale Interessen, europäische Koordinationsmechanismen und institutionelle Pfadabhängigkeiten umfasst, dienen in dieser Masterarbeit die Theorie der „Coordinative Europeanisation“, die Theorie der „Open Method of coordination“ sowie die Theorie des historischen Institutionalismus als theoretische Grundlage. Diese theoretischen Perspektiven ermöglichen es, sowohl die Rolle politischer Diskurse und Expertennetzwerke als auch weiche Formen der EU-Koordination ohne Zwang und die damit einhergehende „policy diffusion“ sowie die Beharrungskraft institutioneller Strukturen in den Blick zu nehmen.

3.1 Sicherheits-Policy Veränderungen durch Krisen – die „Coordinative Europianisation“

“I have always believed that Europe would be built through crises, and that it would be the sum of their solutions.” Jean Monnet (1979)

Die Invasion der Ukraine hat in der EU eine vertiefte und intensivierte Koordinierung zwischen den Mitgliedstaaten sowie zwischen diesen und den europäischen Institutionen ausgelöst. Der russische Angriffskrieg und damit einhergehend auch die Rückkehr des Krieges nach Europa, stellt für die EU eine der größten Krisen ihrer Geschichte dar. Entgegen früheren Beobachtungen und Annahmen, dass außenpolitische Krisen zu einer vermehrten Nationalisierung der Außenpolitik der einzelnen Mitglieder führen und somit zu einer möglichen Zersplitterung der EU-Außenpolitik, hat diese Krise vertiefte Kooperation und Koordination in verschiedenen Bereichen der Außen- und Sicherheitspolitik ausgelöst. In der Theorie der Europäisierung der Außen- und Sicherheitspolitik lassen sich im Wesentlichen zwei Anpassungsprozesse bei den Politiken der Mitgliedstaaten unterscheiden. Diese sind die vertikale Integration, auch bekannt als „down-loading“, also das Übernehmen von EU-Policies,

Strukturen, Normen und Strategien auf die nationale Ebene, und die horizontale Integration, bei der Policies, Normen und Strategien von anderen Staaten im Sinne der Europäisierung übernommen werden. Die horizontale Integration ist auch als „cross-loading“ bekannt und beschreibt eine Situation, bei der Mitgliedsstaaten von anderen Mitgliedern lernen. (Juncos u. a. 2025, 121–23) Dass außenpolitische Krisen zu vertiefter Koordination in der gemeinsamen Außenpolitik führen, konnte in der bestehenden Literatur bislang nicht regelmäßig gezeigt werden. Im Bereich der Sicherheits- und Außenpolitik konnten Autoren in der Vergangenheit eher erkennen, dass Krisen zu einer verstärkten Nationalisierung und zu einer verstärkten De-Europäisierung geführt haben. Als Beispiel für hierfür kann die Flüchtlingskrise im Mittelmeerraum herangezogen werden. Diese hat dazu geführt, dass die italienische Regierung im Alleingang die Seerettungsmission „Mare Nostrum“ gestartet hat und somit aufgaben übernommen hat, die in den Aufgabenbereich von Frontex fallen. (Tassinari 2016)

Ob Krisen zu vermehrter Kooperation führen oder zu einer vermehrten De-Europäisierung, hängt oft damit zusammen, in welchem Ausmaß Länder von einer Krise betroffen sind und ob die Problemlösungskompetenzen in dem zugehörigen Politikfeld bei der EU liegen. Eine Krise, von der alle Mitgliedsstaaten im gleichen Ausmaß betroffen sind und bei der die meisten Entscheidungskompetenzen bereits zum Zeitpunkt des Ausbruchs auf der Ebene der EU liegen, ist daher anders zu beurteilen als eine Krise, die nur einzelne Mitgliedsstaaten betrifft und bei der es keine Kompetenzen auf Ebene der EU gibt. So sind beispielsweise die EU-Mitglieder von der Flüchtlingskrise 2015/16 unterschiedlich betroffen gewesen und die EU hat im Bereich der Migrationspolitik nur über begrenzte Entscheidungskompetenzen verfügt. Im Bereich der Migration obliegt nach wie vor der überwiegende Teil der Entscheidungen den nationalen Regierungen. Durch diese Kombination ist es zu nationalstaatlichem Dissens sowie Blockaden auf EU-Ebene gekommen. Dies führt in weitere Folge zu einem intergouvernementalen Ringen in einem hoch politisierten Umfeld. Eine solche Situation kann auch zu nationalen Alleingängen führen. (Ferrara und Kriesi 2022, 1357–60) Internationale Krisen können unterschiedliche Länder unterschiedlich hart treffen. Eine Außenpolitische Krise, die für ein Mitglied existenzbedrohend ist, kann für ein anderes Land kein Problem beziehungsweise nur ein kleines Problem darstellen. Für das betroffene Lande ist eine Veränderung und Anpassung

der Außenpolitik dringend notwendig, während diese Notwendigkeit für das weniger betroffene Land nicht besteht und ein Festhalten am Status Quo bevorzugt wird, weil eine Veränderung Nachteile mit sich bringen würde. Dies kann in weiterer Folge dazu führen, dass weniger betroffene Staaten gemeinsame europäische Lösungen aktiv blockieren. Aus diesem Gründen bemühen sich besonders von Krisen betroffene Staaten oft um multilaterale Lösungen und Verhandlungen mit anderen Staaten oder um nationale Lösungen. Durch dieses Verhalten wird die Krise nicht auf der europäischen Ebene gelöst und es kommt zu keiner verstärkten europäischen Integration. (Lehne 2022)

Die russische Invasion der Ukraine hat im Jahr 2022 für alle europäischen Staaten eine umfassende Krise ausgelöst. Neben dem Politikfeld der Außen- und Sicherheitspolitik hat es auch in weiteren Politikfeldern Krisen gegeben. So zum Beispiel im Feld der Energie- und Wirtschaftspolitik infolge der gestiegenen Gaspreise sowie der Sanktionen gegen Russland und im Feld der Migrationspolitik aufgrund der massiven Fluchtbewegung von Ukrainern in die angrenzenden EU-Länder. Aufgrund dieser Krisen hat es insbesondere zu Beginn der Krise ein starkes Gefühl der Einheit und der Solidität gegeben und die Mitgliedsstaaten sind offen für Veränderungen und Anpassungen gewesen. (Juncos u. a. 2025, 119) Im weiteren Verlauf des Ukraine-Krieges sind die europäischen Staaten immer häufiger von russischen Desinformationskampagnen, insbesondere im Vorfeld nationaler Wahlen, betroffen gewesen. Die ausländische Beeinflussung nationaler Wahlen sowie der, in Kapitel zwei beschriebene, Verlust der nationalen Souveränität stellt zunächst nur eine nationale Krise für die jeweiligen Mitgliedsstaaten dar und keine europäische. Da aber nationale Wahlen sowie die Meinungen der nationalen Bevölkerung einen Einfluss auf die Prozesse, die Institutionen und die Handlungsmöglichkeiten der EU haben können, kann sich ein zuerst nationales FIMI-Problem rasch zu einer EU-weiten Krise mit Auswirkungen auf die gesamte europäische Integrationsdynamik und die Handlungsmöglichkeiten der Mitglieder insbesondere im Bereich der Außen- und Sicherheitspolitik entwickeln. (Pichler 2024)

Die Theorie der „coordinative Europeanisation“ kann auch im Bereich der FIMI-Policy eine Anwendung finden. Ebenso wie die Ukraine Krise ist FIMI ein Problem, von dem alle EU-Mitgliedsstaaten betroffen sind, wenn auch in unterschiedlicher Intensität. FIMI ist aber auch eine Problematik, die viele verschiedene Policy-Bereiche, wie zum Beispiel Wahlen, Migration

oder Gesundheit betrifft. Dadurch lässt sich argumentieren, dass die beiden Bedingungen, die symmetrische Betroffenheit der Mitgliedsstaaten sowie der große politische Wirkungsbereich, die laut Juncos et al. (2025) die „coordinative Europeanisation“ im Rahmen der Ukraine Krise möglich gemacht haben, auch im Bereich der FIMI-Bedrohungen gegeben sind. Die gemeinsame Bedrohung durch FIMI hat unter anderem dazu geführt, dass gemeinsame Maßnahmen wie die FIMI-Toolbox oder das „Rapid Alert System“ eingeführt worden sind. Auch gibt es nun vermehrte Zusammenarbeit zwischen den Mitgliedsstaaten und EU-Institutionen wie dem EEAS. Hierbei zeigt sich, dass die Maßnahmen gegen FIMI in großen Teilen nicht „Top-Down“ implementiert worden sind, sondern, dass sich die Mitgliedsstaaten in informellen Rahmen koordiniert haben. (Juncos u. a. 2025) Des Weiteren zeigt sich am Prozess der FIMI-Policy auch, dass Staaten, die über langjährige Erfahrung mit FIMI-Abwehr verfügen, wie Schweden mit der psychologischen Verteidigungsagentur oder Frankreich mit VIGINUM, siehe Kapitel 7, eine agendasetzende Rolle einnehmen und anderen Staaten bei der Verbesserung ihrer Fähigkeiten und Kapazitäten helfen. Eine ähnliche Rolle wird von Juncos et al. (2025) den osteuropäischen Mitgliedsstaaten im Zusammenhang mit der Ukraine-Krise zugeschrieben. Die geografische Nähe zu Russland sowie die historische Erfahrung als Mitglieder des Warschauer Pakts verschaffen diesen Staaten ein vertieftes Verständnis des russischen Militärs und der politischen Strukturen Russlands. (Juncos u. a. 2025) Somit geht im Rahmen der FIMI-Bedrohung die weitere Integration nicht nur von den üblichen Treibern für vertiefenden Integration, Frankreich und Deutschland, aus. Die geteilte Bedrohungswahrnehmung führt dazu, dass auch kleinere Staaten ihre Expertise in die Koordinationsbemühungen einbringen.

Durch das Konzept der „coordinative europeanisation“ ist der strategische Kompass der EU für Sicherheit und Verteidigung geschaffen worden, der darauf abzielt, die Verteidigungsfähigkeiten der EU für die Zukunft zu stärken. Zunächst ist im Rahmen der deutschen Ratspräsidentschaft 2020 unter Einbeziehung aller Nachrichten- und Geheimdienste eine 360 Grad-Bedrohungsanalyse erstellt worden. Basierend auf dieser Analyse ist anschließende der Strategische Kompass in einem gemeinsamen Prozess der Mitgliedstaaten erstellt worden. Hierbei haben die europäischen Institutionen, in Funktion des Hohen Vertreters für Außen- und Sicherheitspolitik, die Rolle als Koordinierungsunterstützung

eingenommen. Die Inhaltlichen Schwerpunkte und die Policies sind durch die Mitgliedstaaten beigetragen worden. (Kaim und Kempin 2022) Im März 2022, wenige Wochen nach dem Beginn des russischen Angriffskriegs auf die Ukraine, wurde der Strategische Kompass der EU schließlich veröffentlicht. In diesem Strategiepapier bekennen sich die EU und die Mitgliedsstaaten unter anderem dazu, im Bereich von FIMI vermehrt zusammenzuarbeiten und gemeinsam die bestehenden Methoden zur Erkennung und Analyse zu verbessern. In diesem Dokument bekennen sich die Staaten der EU auch dazu, die gesellschaftliche Resilienz gegen FIMI zu erhöhen. Die Wahrnehmung einer gemeinsamen Bedrohungslage hat dazu geführt, dass es in Bereichen, in denen es bislang nur eine geringe Kompetenz auf der EU-Ebene gegeben hat, zu Policy-Veränderungen und vermehrter Koordinierung gekommen ist. (European Union 2022)

3.2 Policy Änderungen durch Lerneffekte von anderen Staaten – Die „Offene Methode der Koordinierung“ Lesson learning policy drawing.

Die „Offene Methode der Koordinierung“ (OMK) wurde im Rahmen des Europäischen Rat in Lissabon 2000 als eine neue Governance-Methode innerhalb der EU eingeführt. Die OMK verfolgt das Ziel, politische Reformen und Koordination in diversen Politikfeldern zu erreichen, ohne dabei auf verbindliche EU-Rechtsakte zurückgreifen zu müssen. Ein zentrales Element der OMK ist das „Policy learning“. Dieses besagt, dass die Mitgliedsstaaten ihre Problemlösungen und Strategien durch verbesserten Wissensaustausch, Erfahrungsaustausch und „best-practice“ Beispielen aus anderen Staaten, verbessern. Es handelt sich hierbei also um eine lernbasierte Governance-Struktur bei der die Mitglieder durch Peer-Reviews, Benchmarking und Monitoring voneinander lernen und somit eine Basis haben, ihre jeweiligen nationalen Policies zu verbessern. (Radaelli 2003, 9–12) Eine weitere entscheidende Charakteristik der OMK ist die Freiwilligkeit. Staaten verändern ihre Policies und Methoden nicht aufgrund zwingender rechtlicher Verpflichtungen, sondern auf der Basis von normativen Vorstellungen und freiwilligen politischen Zusagen. Bei der OMK handelt es sich also um eine Art des so genannten „Soft-law“. Somit steht die OMK im Gegensatz zu den europäischen Verträgen sowie den europäischen Richtlinien und Verordnungen, welche auch als „Hard-law“ bezeichnet werden und von den Staaten verpflichtend umgesetzt werden müssen. Durch das Aufbauen von Druck können Staaten Policy Veränderungen in anderen Mitgliedsstaaten

allerdings wahrscheinlicher machen. Dieses Konzept wird auch „naming und shaming“ bezeichnet (Zeitlin 2005, 30)

Bei der OMK werden zuerst auf Ebene der EU gemeinsam Leitlinien und Zielsetzungen definiert. Diese werden dann durch die einzelnen Mitgliedsstaaten in eigene nationale Pläne, Maßnahmen und Strategien umgesetzt. Die nächsten Schritte der OMK sind regelmäßige Evaluierungen der Fortschritte, der Vergleich von Kennzahlen sowie das Besprechen der jeweiligen nationalen Pläne in Peer-Reviews. Hierbei ist besonders hervorzuheben, dass es weder einen klaren hierarchischen Top-Down Ansatz noch einen eindeutigen Bottom-Up Ansatz gibt, sondern, dass Lernprozesse durch Kooperation und Austausch unter den Mitgliedsstaaten zu Stande kommen. Radaelli (2003) schreibt hierzu, dass es stets in einem der Mitgliedsländer, eine Lösung für ein bestimmtes Problem gibt, diese Lösung aber nicht Top-Down gefunden werden kann. Die OMK funktioniere daher wie eine Art Radar, dass potenzielle Lösungen sowie politische Innovation aufdeckt und somit für alle Staaten sichtbar macht. Des Weiteren unterscheidet Radaelli zwischen zwei Formen des Lernens. Das kognitive Lernen und das normative Lernen. Bei der Form des kognitiven Lernens verstehen Staaten die Ursache-Wirkungszusammenhänge bestimmter politischer Maßnahmen und können ihre nationalen Policies basierend auf diesen Erkenntnissen anpassen. Beim normativen Lernen werden hingegen Werte sowie die Vorstellung, wie sich gute Politik manifestieren soll, von anderen Staaten übernommen. In der OMK werden diese beiden Arten des Lernens zusammengebracht. (Radaelli 2003, 24–25) Das ideale Ergebnisse der OMK ist die „ideational convergence“. Hierbei handelt es sich um eine Situation, bei der sich die die Vorstellungen und die Ideen über erfolgreich policies zwischen den Staaten immer weiter angleichen und am Ende ein ähnliches Verständnis von guter Politik besteht. Das heißt allerdings nicht, dass sich die Policies, die auf nationaler Ebene umgesetzt werden, zwingend angleichen. In diesem Kontext würde man von „policy convergence“ sprechen. (Radaelli 2003, 45–47) Insgesamt handelt es sich bei der OMK also um ein Werkzeug, welches laut Radaelli großes Potential hat und viele Verbesserungen hervorbringen kann. Die Lerneffekte sind allerdings meist nur Oberflächlich, weil nationale Eigeninteressen sowie fehlende Partizipation der Mitgliedstaaten und fehlende institutionelle Einbettung der OMK Lernerfolge verhindern und behindern. (Radaelli 2003, 45–46)

Für Gewöhnlich wird die OMK vor allem in den Bereichen der Beschäftigungs-, Bildungs,- Arbeits-, und Innovationspolitik angewandt. Die OMK kann auch im sehr sensiblen Bereich der Migrations- und Integrationspolitik Anwendung finden. Dies sind Bereiche mit sensiblen nationalen Unterschieden und unterschiedlichen nationalen Präferenzen, bei denen ein „Top-down“ Ansatz auf Widerstand aus den nationalen Bevölkerungen stoßen würde und daher das Konzept der Freiwilligkeit benötigt wird. (Radaelli 2003, 16–17) Im Bereich der Sicherheits- und Verteidigungspolitik wird die OMK in der Regel nicht angewandt. Hierbei handelt es sich um Politikbereichen, die üblicherweise die nationale Souveränität betreffen und daher der Gedanke der Integration im Vordergrund steht. In diesen Politikbereichen stützen sich die Mitgliedsstaaten also eher auf verbindliche Kooperationsformate wie die „permanent and structured cooperation“ PESCO, an der mit der Ausnahme von Malta alle EU-Mitgliedsstaaten teilnehmen. Allerdings lässt sich die OMK bei einigen Themen und Politikfeldern im Nahbereich der Sicherheits- und Verteidigungspolitik anwenden, bei denen Koordination und Wissensaustausch von Vorteil sind. Im Bereich der FIMI-Abwehr bietet die OMK einen angemessenen und systematischen Rahmen zur Koordination und vereinfacht den Austausch von Best-Practice Methoden in den Bereichen Risiko- und Datenanalyse, der Erkennung von Desinformationskampagnen und der Stärkung der Resilienz der Bevölkerung. Des Weiteren hilft der verbesserte Austausch von Geheimdienstinformationen bei der Verteidigung. (D’Andrea u. a. 2025)

Im Bereich der Verteidigung gegen FIMI wurde im Jahr 2019 vom EEAS das „Rapid Alert System“ (RAS) eingerichtet. Hierbei handelt es sich um ein Netzwerk welches aus den 28 europäischen Mitgliedsstaaten, digitalen Plattformen und Fakten Checkern besteht. In diesem Netzwerk werden Informationen zu Desinformation, spezifischen FIMI-Kampagnen und Möglichkeiten zur Steigerung der Resilienz unter den Mitgliedern ausgetauscht. Des Weiteren werden im RAS auch die Koordination der gemeinsamen Verteidigung und die gemeinsame strategischen Kommunikation abgesprochen. Dieses Netzwerk trifft sich regelmäßig zum Austausch von „Best-Practice Policies“, Analysen und Berichten. (EEAS 2024a, 13–15) Durch das RAS wird die Wichtigkeit multilateraler Zusammenarbeit zur Begegnung von Desinformation unterstrichen. FIMI ist ein Sicherheitsproblem, das in der Grauzone zwischen innerer und äußerer Sicherheit stattfinden. In diesem Bereich könnte eine klassische

verbindliche Regulierung auf nationale Widerstände aufgrund von nationalen Sicherheitsbedenken, Bedenken bezüglich Einschränkung der Meinungsfreiheit oder Medienfreiheit stoßen. Durch den freiwilligen Charakter der OMK innerhalb des RAS können die Staaten im Bereich der FIMI-Abwehr zusammenarbeiten, ohne dass Kompetenzverluste befürchtet werden müssen. Weiters lassen sich die rapiden Veränderungen der FIMI-Bedrohungen gut mit dem adaptiven Charakter der OMK vereinbaren. Somit stellt dieses Netzwerk ein erfolgreiches Beispiel der OMK im Bereich der FIMI-Abwehr dar und hilft dabei, die kollektive Sicherheitsarchitektur in der EU zu stärken. (D'Andrea u. a. 2025)

3.3 Historischer Institutionalismus

Eine weitere Theorie, mit der sich die Policy-Änderungen und Entwicklungen von Institutionen innerhalb von Staaten erklären lassen, ist der historische Institutionalismus. Im Grunde genommen besagt der historische Institutionalismus, dass die Handlungen und Entscheidungen von politischen Akteuren durch die Institutionen, in denen ihr Handeln stattfindet, bestimmt sind. Diese Institutionen sind allerdings mehr als nur bloße Rahmenbedingungen oder Spielregeln, sondern Normen und Werte, die beeinflussen welche Handlungsoptionen politische Akteure als möglich oder angemessen wahrnehmen können. Im historischen Institutionalismus sind Institutionen verschiedene Arten von Organisationen, die formalen und informellen Regeln unterworfen sind. Zu diesen können, neben den staatlichen Institutionen, auch wirtschaftliche Organisationen oder Gewerkschaften zählen. Politische Akteure entscheiden über die Ergebnisse von politischen Handlungen und da Institutionen die Werte, Strategien und Wahrnehmungen der politischen Akteure beeinflussen, haben Institutionen auch einen direkten Einfluss auf die politischen Ergebnisse und mögliche Veränderungen. (Hall und Taylor 1996)

Ein Kernelement dieser theoretischen Schule ist die Pfadabhängigkeit. Diese besagt, dass zu einem früheren Zeitpunkt getroffene Entscheidungen und die damit einhergehende Beschaffenheit von Institutionen, starken Einfluss darauf haben, welche Entscheidungen zu einem späteren Zeitpunkt getroffen werden und wie diese Entscheidungen oder Veränderungen ausgestaltet sind. (Hall und Taylor 1996) Pfadabhängigkeit entsteht durch verschiedene Erklärungsmechanismen, die dazu führen, dass einmal eingeschlagene

institutionelle Entwicklungspfade mit der Zeit stabiler und schwerer zu verändern sind. Ein zentraler Mechanismus hierfür ist das Konzept der „increasing returns“. Dieses besagt, dass früher getroffene Entscheidungen zukünftige Entwicklungen wahrscheinlicher machen, da mit der Zeit steigende Vorteile oder sinkende Veränderungsanreize entstehen. Institutionen wirken dabei selbstverstärkend. Je länger sie bestehen, desto größer werden die politischen und organisatorischen Kosten eines Kurswechsels. (Pierson 2000) Ein zweiter Mechanismus ist das Konzept der „adaptiven Erwartungen“. Menschen und Organisationen treffen ihre Entscheidungen zunehmend in der Annahme, dass bestehende Institutionen auch künftig in ihrer heutigen Form bestehen bleiben. Diese Erwartung stabilisiert Institutionen zusätzlich, da sich individuelle und kollektive Strategien entsprechend anpassen und angleichen. Hierzu kommen auch noch so genannte Netzwerkeffekte, bei denen der Nutzen des Individuums steigt je mehr andere Menschen aus einer bestimmten Institution einen Nutzen ziehen. Damit geht auch der Effekt der Lernerfahrungen einher. Dieser Effekt besagt, dass Menschen im Verlauf der Zeit Wissen zu einer Institution erwerben und somit für sich selbst aus dieser Institution höhere Gewinne erzielen. Ein zusätzlicher Grund für Pfadabhängigkeit liegt in den steigenden politischen Kosten, die mit einer Abkehr vom bestehenden institutionellen Pfad verbunden sind. Während sich institutionelle Arrangements zunehmend verfestigen, sinkt die Wahrscheinlichkeit, dass politische Alternativen ernsthaft in Betracht gezogen werden. Auch dann, wenn sie sachlich überlegen wären. Somit kann Pfadabhängigkeit dazu führen, dass suboptimale Politiken fortgeführt werden, weil ein Umstieg mit hohen politischen, sozialen oder wirtschaftlichen Kosten verbunden wäre. (Pierson 2000)

Die Schule des historischen Institutionalismus geht davon aus, dass Policy-Veränderungen in der Regel nur inkrementell und in Nuancen geschehen. Größere Veränderungen werden vor allem umgesetzt, wenn es zu so genannten „critical junctures“ kommt. Dies sind wichtige und große Ereignisse, die einen vollständigen Paradigmenwechsel zur Folge haben und notwendig machen. Solche „critical junctures“ können zum Beispiel Wirtschaftskrisen, Kriege oder andere exogene Schocks sein, zu deren Bewältigung eine komplett neue Lösung umgesetzt werden muss und die ein Abweichen von bisher bewährten Pfaden möglich machen. Auch abseits von der Mechanik der „critical junctures“ können sich im historischen Institutionalismus Policy-Veränderungen durch andere Mechaniken ergeben, die insbesondere im Fall der europäischen

FIMI-Verteidigung relevant sind. So gibt es die Mechanik des „layering“. Bei dieser Mechanik werden neue Regeln und Systeme ergänzend zu bereits bestehenden hinzugefügt oder daraufgelegt. Des Weiteren gibt es die Mechanik der „conversion“. Bei dieser werden bestehende Systeme umfunktioniert, sodass sie zur Lösung neuer Probleme eingesetzt werden können. Bei diesen beiden Mechaniken werden die alten Systeme beibehalten. (Mahoney und Thelen 2009) In der FIMI-Abwehr sind diese beiden Mechaniken beispielsweise relevant, da man zum Beispiel Cybersicherheitsagenturen oder Geheimdiensten zusätzliche Aufgabenbereiche überlassen oder bereits bestehende Möglichkeiten zur strategischen Kommunikation mit der Bevölkerung für die strategische FIMI-Kommunikation nutzen kann. So basiert beispielsweise die FIMI-Toolbox, die im nächsten Kapitel beschrieben wird, auf der „EU Hybrid-Toolbox“ und ist dieser sehr ähnlich.

Die russische Vollinvasion der Ukraine und die damit einhergehende hybride Kriegsführung gegen die europäischen Staaten kann als „critical juncture“ in Betracht gezogen werden. Durch diese Krise werden Staaten dazu gebracht von den etablierten Pfaden abzuweichen und neue Policies und Institutionen zu etablieren. Mit dem Erklärungsansatz der Pfadabhängigkeit lässt sich des Weiteren erklären, warum sich die Policies zur FIMI-Verteidigung verschiedener Staaten unterscheiden. Staaten befinden sich auf unterschiedlichen institutionellen Pfaden und haben daher unterschiedliche Ausgangslagen im Bereich der Verteidigung. So hat Schweden eine lange Geschichte im Bereich der so genannten psychologischen Verteidigung und im Bereich der „digital-literacy“. Die Pfadabhängigkeit kann daher erklären, warum man sich in Schweden für den Ansatz der totalen Verteidigung entschieden hat. In der Fallstudie zur schwedischen FIMI-Abwehr in Kapitel 7 wird näher darauf eingegangen.

4 Europäischen Maßnahmen, Initiativen und Pläne

Wie bereits in den vorherigen Kapiteln angesprochen, werden viele Beschlüsse und Initiativen im Bereich der FIMI-Abwehr auf der europäischen Ebene getroffen. Die Europäische Kommission hat in den vergangenen Jahren eine Vielzahl an technischen, institutionellen und zivilgesellschaftlichen Maßnahmen zur FIMI-Bekämpfung und zum Schutz der Bevölkerung erlassen. In diesem Kapitel werden die verschiedenen Maßnahmen sowie ihre Funktionsweise beschrieben.

Institutionell ist die FIMI-Abwehr auf der europäischen Ebene innerhalb der Gemeinsamen Sicherheits- und Verteidigungspolitik (GSVP) angesiedelt. Die GSVP wiederum ist Teil der Gemeinsamen Außen- und Sicherheitspolitik (GASP), die im Rahmen des Vertrags von Maastricht 1993 beziehungsweise im Vertrag von Nizza 2001 eingeführt worden ist. (EEAS 2024a) Diese beiden Politikfelder zeichnen sich dadurch aus, dass das Europäische Parlament und die Europäische Kommission nur über wenig Mitspracherechte und Entscheidungskompetenzen verfügen und daher die Mitgliedsstaaten im Rahmen des Europäischen Rates die meisten Entscheidungen treffen. Die Entscheidungen sind den Regeln des Europäischen Rates unterworfen, wobei hier meist das Einstimmigkeitsprinzip gilt. Sicherheits- und verteidigungspolitische Maßnahmen und gemeinsame Reaktionen auf diverse hybride Bedrohungen bedürfen daher breiter politischer Zustimmung zwischen den Mitgliedsstaaten. Somit sind die Policies und Strategien zur FIMI-Abwehr stark durch intergouvernementale Koordinierung und Konsens zwischen den Mitgliedern beeinflusst, was in weiterer Folge dazu führen kann, dass es in Krisenzeiten zu Verzögerungen und gegenseitigen Blockaden aufgrund unterschiedlicher nationalstaatlicher Interessen kommt. (Bayer u. a. 2021)

Im Rahmen ihrer regulatorischen Bemühungen hat sich die EU in erster Linie auf vier unterschiedliche Ansätze beziehungsweise Politikbereiche zur Bekämpfung von FIMI-Kampagnen gestützt. Diese sind die Außenbeziehungen der EU, die Grundrechte, die „Media-Literacy“ sowie die Regulierung beziehungsweise Selbstregulierung von großen Online-Plattformen. In ihren Bemühungen im Kampf gegen FIMI befindet sich die EU stets in einem Spannungsfeld. Zum einen möchte und sollte man die Meinungs- und Redefreiheiten der EU-Bürger nicht grundlos einschränken und zum anderen ist es das erklärte strategische Ziel, den Schutz der demokratischen und rechtsstaatlichen Ordnung sowie der staatlichen Souveränität zu gewährleisten. (Kachelmann und Reiners 2023)

4.1 Maßnahmen im Rahmen der EU-Außen- und Sicherheitspolitik

Da ein beachtlicher Anteil der europäischen Reaktion auf FIMI-Bedrohungen im Rahmen der gemeinsamen Außenpolitik geschieht, übernimmt der EEAS eine Führungsrolle in der Abwehrarbeit. Die Entscheidung der EU, die FIMI-Bedrohung gemeinsam mit anderen

hybriden Bedrohungen als Sicherheitsproblem einzuordnen, wurde im Rahmen des Europaratsbeschlusses im März 2015, ein Jahr nach der Besatzung der Krim-Halbinsel durch Russland, getroffen. Die Mitgliedsstaaten haben den damaligen EU-Außenbeauftragten dazu aufgefordert, einen Aktionsplan für die strategische Kommunikation zu erstellen, mit dem man sich gegen zukünftige russischen Desinformationskampagnen verteidigen kann. Dieser Fokus auf die Abwehr von Desinformation aus dem Ausland, hat insbesondere zu Beginn der europäischen Abwehrbemühungen den Nebeneffekt gehabt, dass nur wenig gegen die Verbreitung von Desinformation und FIMI durch Akteure innerhalb der EU unternommen worden ist. (Proto u. a. 2025)

Als eine der ersten europäischen Maßnahmen wurde im Jahr 2015 die „EAST StratCom Task Force“ innerhalb des EEAS gegründet. Diese Task Force hat den Auftrag, Kommunikationsstrategien zu entwickeln, um russlandfreundlicher Desinformation und pro-russischer Propaganda entgegenzuwirken. Die Aufmerksamkeit der Task Force richtet sich dabei primär auf die osteuropäischen EU-Mitgliedsstaaten und andere, ehemals zur Sowjetunion gehörende Staaten, wie Moldawien, Georgien und die Ukraine. (von Salzen 2015) Diese Task Force hat unter anderem die „EUvsDesinfo“ Datenbank aufgebaut und öffentlich zugänglich gemacht. In dieser Datenbank sind mehr als 15.000 Einträge zu russischer Desinformation verfügbar. Mit dieser Datenbank lassen sich Muster und häufig wiederholte Narrative der russischen Desinformation erkennen und analysieren. Darüber hinaus hat EUvsDesinfo basierend auf den eigenen Erkenntnissen Lerninhalte zur Stärkung der Media-Literacy erstellt, die ebenso öffentlich verfügbar sind. (D’Andrea u. a. 2025) Die EUvsDesinfo Datenbank ermöglicht eine faktenbasierte strategische Kommunikation, um die Bevölkerung vor Desinformationskampagnen zu warnen.

Ein elementarer Bestandteil der europäischen Verteidigung gegen FIMI und wichtiges Werkzeug im Kampf gegen koordinierte ausländische Desinformation ist die vom EEAS entwickelte FIMI-Toolbox. Die FIMI-Toolbox ist unter anderem im Rahmen der EU-Parlamentswahlen im Jahr 2024 zum Einsatz gekommen, um russische Einflussnahmen zu unterbinden. Diese Toolbox lehnt sich an die EU Hybrid-Toolbox an und ist komplementär zu dieser zu verstehen und einzusetzen. Es handelt sich hierbei nicht um eine rein technische Maßnahme, sondern um einen institutionalisierten Maßnahmenkatalog. Dieser erlaubt es der

EU flexibel und koordiniert auf einzelne Bedrohungen zu reagieren. Der Aufbau der FIMI-Toolbox ist dreistufig. In der ersten Ebene werden Daten zu FIMI-Vorfällen gesammelt, strukturiert und analysiert. In der zweiten Ebene werden diese Erkenntnisse innerhalb eines methodischen Rahmens bewertet. Bewertet werden hierbei die Herkunft, die Mittel, die Ziele sowie die Auswirkungen eines einzelnen FIMI-Vorfalles. In der dritten Ebene werden, basierend auf den Erkenntnissen der zweiten Ebene, entsprechende Maßnahmen erlassen. Zu diesen gehören diplomatische Erklärungen, Sanktionen, strategische Kommunikation, gezielte Aufklärungskampagnen oder technische Hilfeleistungen für andere. In der FIMI-Toolbox sind Maßnahmen inkludiert, die kurz-, mittel- und langfristig eingesetzt werden können und die sowohl zur Reaktion auf spezifische FIMI-Vorfälle als auch zur generellen Prävention geeignet sind. (EEAS 2024b, 12–14)

Die in der FIMI-Toolbox aufgelisteten Maßnahmen sind in vier grundsätzliche Kategorien unterteilt. Die erste ist die „Situational Awareness“. Hierbei handelt es sich um das grundlegende Verständnis für die FIMI-Bedrohung. Dieses ist notwendig, um zu entscheiden welche Reaktion auf einen spezifischen FIMI-Vorfall angemessen ist. Die zweite Kategorie ist das „Resilience Building“. Die Maßnahmen dieser Kategorie inkludieren unter anderem, dass man in der Bevölkerung ein Bewusstsein für die Desinformationsproblematik schafft und, dass man bereits frühzeitig mit der entsprechenden strategischen Kommunikation beginnt. Die Maßnahmen dieser Kategorie sind primär präventiver Natur. Die dritte Kategorie ist jene der „Disruption and Regulation“ und hierbei geht es darum, dass man durch neue Gesetze und Richtlinien die Verbreitung von FIMI einschränkt beziehungsweise erschwert. Mit diesen Maßnahmen wird darauf abgezielt, den Verbreitern von FIMI die dazu notwendigen Plattformen und Kanäle zu entziehen. Zu den Maßnahmen dieser Kategorie zählen unter anderem bestimmte Aspekte des „Digital Service Act“ (DSA) der EU, mit dem unter anderem große Internet-Plattformen dazu verpflichtet werden gewisse Inhalte zu entfernen, die Betreiber von FIMI-Kanälen zu sperren und für mehr Transparenz zu sorgen. Die vierte Kategorie ist die „EU External Action“. Zu dieser Kategorie gehören auch Maßnahmen im Rahmen der Gemeinsamen Außen- und Sicherheitspolitik (GSVP) und diplomatische Maßnahmen. (EEAS 2024b) Mithilfe von Maßnahmen aus dieser Kategorie kann man Sanktionen gegen bestimmte Personen, Organisationen und Unternehmen erlassen. So sind

zum Beispiel die Kanäle der russischen Medienunternehmen RT und Sputnik in der EU verboten worden und Einreiseverbote gegen einzelne FIMI verbreitende Personen erlassen worden. (Cenusa 2024; European Council 2024) In der folgenden Grafik sind die vom EEAS erdachten Maßnahmen sowie deren Kategorien angeführt. Diese Maßnahmen werden regelmäßig erweitert und verbessert.

Abbildung 2 EEAS 2024 2. FIMI-Report - FIMI-Toolbox

4.2 HWP ERCHT

Die „Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats“ (HWP ERCHT) ist ein Gremium im Rat der EU, welches 2019 gegründet wurde, um einen bereichsübergreifenden Ansatz im Umgang mit hybriden Bedrohungen einschließlich FIMI

sicherzustellen. Diese Arbeitsgruppe soll die Abstimmung und die Kooperation zwischen den Mitgliedsstaaten sicherstellen. Im FIMI-Bereich liegt der Fokus insbesondere auf der Bildung von Resilienz und der Erarbeitung gemeinsamer strategischer Kommunikation, um Desinformationsnarrativen und -kampagnen entgegenzutreten. So werden im Rahmen dieser Arbeitsgruppe Leitfäden, Frühwarnsysteme und Koordinationsmechanismen organisiert. Auch wenn die Mitgliedsstaaten im Rahmen der HWP ERCHT miteinander kooperieren, obliegt die Verantwortung für die nationale Sicherheit nach wie vor den Mitgliedsstaaten. (Europäischer Rat 2019) Im Rahmen der HWP ERCHT wird auch mit nicht-EU Mitgliedern wie der NATO oder der Schweiz kooperiert.

4.3 Digital Service Act und Digital Markets Act

Da im Informationszeitalter FIMI-Kampagnen primär über Online-Plattformen, Soziale Netzwerke und Messenger-Dienste verbreitet werden, versucht die EU seit einigen Jahren diese stärker zu regulieren und somit die Verbreitung von Desinformation und FIMI einzuschränken. Eine der ersten Maßnahmen zur Regulierung von Online-Plattformen ist der „Code of Practice on Disinformation“ gewesen. Hierbei handelt es sich um einen freiwilligen Pakt zur Selbstregulierung von Online-Plattformen, dem sich unter anderem Meta, Google und Microsoft angeschlossen haben. Diese Unternehmen haben sich mit dem Pakt dazu verpflichtet, auf ihren Plattformen für mehr Transparenz, mehr Inhaltsmoderation und verstärktes Vorgehen gegen Bot-Netzwerke zu sorgen. Basierend auf diesem freiwilligen Pakt, ist später der Digital Service ACT (DSA) beschlossen worden. (Bayer 2024)

Im November 2022 ist der DSA gemeinsam mit dem Digital Markets Act (DMA) in Kraft getreten. Die meisten Bestimmungen sind allerdings erst im Jahr 2024 in Kraft getreten. Ziel dieser beiden Verordnungen ist eine europaweit einheitliche Regulierung sozialer Netzwerke, digitaler Plattformen und online Dienstleister. Des Weiteren wird damit auch ein einheitlicher digitaler Wettbewerb in der EU geschaffen und Maßnahmen eingeführt, mit denen man effizienter und europaweit gegen Hass im Netz und Desinformation und damit in weiterer Folge auch gegen FIMI vorgehen kann. (BMJ 2022) Da es sich beim DSA und beim DMA um Verordnungen handelt, müssen diese Gesetze von den Mitgliedsstaaten nicht in nationales Recht übertragen werden und gelten somit unmittelbar ab Inkrafttreten.

Auch wenn es nicht das primäre Ziel des DSA ist, einen rechtlichen Rahmen für das Vorgehen gegen FIMI zu schaffen, spielt diese Verordnung beim Kampf gegen FIMI und Desinformation eine zunehmend wichtigere Rolle. Der Begriff Desinformation selbst wird in den Gesetzesartikeln nicht explizit erwähnt oder definiert. Desinformation ist im DSA ein gesellschaftliches und systemisches Risiko, wogegen „very large online plattforms“ (VLOP) und „very large online search engines“ (VLOSE) gemäß Artikel 34 und 35 vorgehen müssen. VLOP und VLOSE sind Plattformen und Suchmaschinenanbieter, die mehr als 45 Millionen aktive Nutzer pro Monat verzeichnen, wie zum Beispiel Google, Amazon oder Netflix. Zu den verpflichtenden Maßnahmen zählt die Analyse von gesellschaftlichen und systemischen Risiken, die Eindämmung der Verbreitung rechtswidriger Inhalte, die Analyse und die Verhinderung von Inhalten, die nachteilige Auswirkungen auf die demokratische Debatte, das gesellschaftliche Zusammenleben sowie die Durchführung von Wahlen haben, und die Verhinderung von Inhalten, die Auswirkungen auf die körperliche und geistige Gesundheit von Personen haben. Zusätzlich zu diesen Verpflichtungen müssen VLOP und VLOSE regelmäßige Transparenzberichte und Werbedatenbanken veröffentlichen sowie Forschern Zugriff auf Plattformdaten geben, damit diese die Verbreitung von Desinformation auf den Plattformen untersuchen können. (Jansen 2024)

Auch wenn mit dem DSA einige Fortschritte im Kampf gegen Desinformation und FIMI gemacht werden, existieren einige Lücken, die das Vorgehen der Behörden erschweren. So gelten die oben angeführten Regeln und Verpflichtungen nur für Plattformen und Suchmaschinen mit mehr als 45 Millionen aktiven Nutzern pro Monat, wovon nur eine kleine Zahl an Plattformen betroffen ist. Somit werden viele kleinere Plattformen, die ebenso für FIMI genutzt werden, von den Regulierungen und Verpflichtungen ausgenommen. (Jansen 2024) So ist beispielsweise die Onlineplattform „4-Chan“, die als eine Wiege der rechtsextremen Q-Anon Bewegung gilt, aufgrund der zu geringen Nutzerzahlen nicht von den Vorgaben für VLOPs betroffen. (Bayer u. a. 2019) Ebenso ist der Messenger-Dienst Telegram, der bei der Verbreitung russischer Desinformationskampagnen eine entscheidende Rolle spielt keine VLOP. (EUvsDisinfo 2025)

Des Weiteren fehlt im DSA eine klare juristische Definition von Desinformation, wodurch den Plattformen ein Interpretationsspielraum überlassen wird, den diese ausnutzen können, um

die eigenen Verpflichtungen zu reduzieren. Da das Monitoring von Desinformation sowie die Inhaltsmoderation mit erheblichen Kosten verbunden sind, ist es aus der Sicht der VLOP-Betreiber und VLOSE-Betreiber nur rational, eine für sie möglichst günstige Definition von Desinformation zu wählen. (Jansen 2024) An dieser Stelle sei jedoch erwähnt, dass Begriff wie Wahrheit und Desinformation juristisch schwer zu definieren sind und daher ein gewisser Spielraum für die Plattformen notwendig ist. (Bayer 2024) Eine weitere Schwachstelle des DSA ist, dass die Verteilung der Kompetenzen unklar geregelt ist. So sind sowohl die Europäische Kommission, die verschieden nationalen Medienaufsichtsbehörden und die Plattformen selbst für die Umsetzung des DSA zuständig. (Jansen 2024)

Neben dem DSA wurde von der EU auch der „digital markets act“ DMA erlassen. Hierbei handelt es sich um ein Gesetz, welches nicht direkt für die Bekämpfung von Desinformation und FIMI erlassen worden ist und das komplementär zum DSA betrachtet werden muss. Während sich der DSA den Inhalten von Online-Plattformen widmet, nimmt sich der DMA primär den Machtstrukturen und der Marktlogik von Online-Plattformen an und soll sicherstellen, dass auch kleinere Online-Plattformen eine Chance auf dem Online-Markt haben. Allerdings bringt der DMA auch einige Aspekte mit, die bei der Bekämpfung von FIMI und Desinformation hilfreich sein können. So ist es zum Beispiel Online-Plattformen nicht mehr erlaubt personenbezogene Daten für Trainingszwecke von KI-Modellen zu verwenden. Dadurch wird es schwieriger gezielte Desinformation für einzelne Zielgruppen zu erstellen. Des Weiteren werden mit dem DMA erhöhte Transparenzauflagen eingeführt, wodurch es schwieriger werden soll, FIMI zu verbreiten. Auch werden Forschenden durch den DMA mehr Zugangsmöglichkeiten zu Plattformdaten zugestanden. (Bayer 2024) Der DMA kann also Desinformations- und FIMI-Dynamiken abschwächen, geht aber nicht gezielt dagegen vor.

Zusammengefasst kann über den DSA und den DMA gesagt werden, dass es sich hierbei um Instrumente handelt, die im Rahmen der EU-Binnenmarktkompetenzen beschlossen worden sind. Insbesondere der DMA ist nicht explizit für die Bekämpfung von Desinformation und FIMI geschaffen worden, sondern erzielt seine Wirkung in diesem Bereich durch Folgewirkungen. (Bayer 2024) Eine erste Untersuchung durch das „NATO Strategic Communications Center of Excellence“ in Riga hat in einem Vorher-Nachher Vergleich gezeigt, dass der DSA von der VLOP Facebook noch nicht wie gefordert umgesetzt wird und, dass es seit der Einführung des DSA

keine signifikante Steigerung bei dem Entfernen von Inhalten mit Desinformation gibt. (Bergmanis-Korāts u. a. 2025) Da allerdings die beiden Verordnungen erst im Jahr 2024 vollumfänglich in Kraft getreten sind, werden sich die tatsächlichen Auswirkungen auf die FIMI- und Desinformationslandschaft sowie die tatsächliche Umsetzung durch die Onlineplattformen erst in Zukunft zeigen. Diese beiden Verordnungen bestätigen allerdings, dass die EU sich dieser Probleme regulativ annehmen möchte und in Zukunft weitere legislative Schritte setzen wird.

4.4 Die digitale Souveränität der EU

Insbesondere seit der deutschen EU-Ratspräsidentschaft im Jahr 2020 möchte die EU die eigene digitale Souveränität erreichen. Man hat erkannt, dass man in der EU im Bereich der digitalen Dienstleistungen von Drittstaaten, insbesondere den USA und China, abhängig geworden ist. Die größten und wichtigsten der digitalen Dienstleister und Online-Plattformen sind im Besitz US-amerikanischer oder chinesischer Unternehmen. Im Sinne der digitalen Souveränität und der europäischen strategischen Autonomie beabsichtigt die EU, diese Abhängigkeiten gezielt zu reduzieren. Auch im Bereich von Desinformation und FIMI spielt die digitale Souveränität eine zentrale Rolle. Die europäische Kommission hat das Recht, großen Technologiekonzernen Regeln und Verpflichtungen aufzuerlegen, wenn diese innerhalb des Binnenmarktes aktiv sein möchten. Die Kommission hat auch in der Vergangenheit gezeigt, dass sie bei Verfehlungen bereit ist, Maßnahmen und Strafen gegen große Technologiekonzerne zu verhängen. Allerdings ist man aufgrund der Abhängigkeiten von Drittstaaten bei der Umsetzung von Maßnahmen stets auf die Duldung Dritter angewiesen und hat selbst nur limitierte Handlungsmöglichkeiten. Vor dem Hintergrund der stetig steigenden systemischen Rivalität zwischen den USA und China kann es in Zukunft schwieriger werden Maßnahmen gegenüber großen Technologiekonzernen durchzusetzen. (Kachelmann und Reiners 2023) Solange es allerdings keine europäischen Alternativen zu ausländischen Dienstleistern und Online-Plattformen gibt, bleibt die digitale Souveränität unerfüllt und die europäischen Staaten bleiben im Online-Raum weiterhin abhängig von ausländischen Dienstleistern. Die damit einhergehenden limitierten Handlungsmöglichkeiten der Kommission und der EU-Mitglieder haben auch Auswirkungen auf die Durch- und Umsetzung

der DSA- und DMA-Verordnungen und somit auch auf die Verteidigung gegen FIMI-Bedrohungen.

5 Sicherheitspolitische und außenpolitische Bedrohungsakteure

"*Only when we will have clarity on the nature of the problem, can we try to define and implement proper responses.*" (EEAS 2024a, 7–8)

Diese Worte hat Josep Borell im Jahr 2023, damals der Hohe Vertreter der EU für Außen- und Sicherheitspolitik, geschrieben und damit deutlich gemacht, dass es zur wirkungsvollen Verteidigung gegen einen Angreifer und dessen Desinformations-Kampagnen sowie zum Schutz der europäischen Bevölkerung notwendig ist, die Vorgehensweisen, Prozesse und Taktiken der Angreifer zu erkennen, zu kennen und zu verstehen. Nur mit einem fundierten Wissen über den Angreifer können Abwehrmaßnahmen zielgerichtet entworfen und umgesetzt werden. Zudem können die Motive der Desinformation verbreitenden Staaten nur dann verstanden werden, wenn man ihre Positionierung innerhalb des internationalen politischen Systems sowie die durch FIMI verfolgten strategischen Ziele betrachtet. (EEAS 2024a)

Dieses Kapitel widmet sich den beiden Hauptbedrohungsakteuren im FIMI-Bereich: Russland und China. Neben diesen beiden gibt es noch weitere Staaten, die FIMI einsetzen, wie den Iran, die Türkei oder Nordkorea. Diese sind allerdings für die europäischen Staaten weniger bedeutend, da die Häufigkeit von FIMI-Angriffen aus und von diesen Staaten wesentlich geringer ist als die Häufigkeit von oder aus Russland und China. Des Weiteren lassen sich die „Verteidigungs-Policies" und Strategien, die zur Verteidigung gegen russische und chinesiche FIMI-Kampagnen entwickelt werden, sowie die aus der Verteidigung gewonnen Erfahrungen, auch auf weitere Staaten übertragen.

Von November 2023 bis November 2024 konnte der EEAS 505 FIMI-Vorfälle aufdecken und registrieren. Dabei wurden 38.000 unterschiedliche, zur Verbreitung genutzte Kanäle auf 28 verschiedenen Plattformen entdeckt. Diesen Kanälen ließen sich 68.000 inhaltliche Beiträge, also Posts, Bilder und Artikel, zuordnen. Die FIMI-Vorfälle zielten auf 90 verschiedene Länder und 322 verschiedene Organisationen und Institutionen ab. Dabei sind die einzelnen FIMI-

Vorfälle and die jeweiligen Landessprachen angepasst worden. Des Weiteren sind die entdeckten Hauptmotive politischer sowie wirtschaftlicher Natur gewesen. Die am meisten betroffenen Länder sind die Ukraine, Frankreich und Deutschland gewesen. Frankreich dürfte aufgrund der olympischen und paralympischen Spiele in Paris und Deutschland aufgrund der häufigen Koalitionsstreitigkeiten (EEAS 2025) Im Vorjahreszeitraum von Anfang Dezember 2022 bis November 2023 wurden durch den EEAS 750 FIMI-Vorfälle registriert. (EEAS 2024a)

5.1 Russland als Bedrohungsakteur

Für Russland und das russische Regime sind FIMI-Kampagnen ein regulärer Bestandteil der militärischen Doktrin. Mit FIMI-Werkzeugen und anderen hybriden Methoden soll der Gegner bereits vor dem Beginn der eigentlichen militärischen Auseinandersetzung so geschwächt sein, dass die Entscheidung auf dem Schlachtfeld, ähnlich der Annexion der Krim-Halbinsel im Jahr 2014, schnell und ohne nennenswerte Verluste von statten geht. Der elementare Unterschied zwischen den Doktrinen westlicher Staaten und der russischen Doktrin ist, dass die russische Doktrin einen permanenten FIMI-Einsatz zur Erreichung politischer und strategischer Ziele vorsieht, während die Doktrin westlicher Staaten von einem solchen permanenten Einsatz absieht und FIMI nur während eines Konfliktes anwendet. Dieses Vorgehen wird von westlichen Autoren als Gerasimov-Doktrin bezeichnet, auch wenn es eine Doktrin mit diesem Namen in Russland nicht gibt. Bei dieser Doktrin werden hybride Mittel eingesetzt, um mittels einer „sharp power“, die sich von dem Konzept der westlichen „soft power“ abgrenzt, ausländische politische Systeme zu penetrieren und die Kontrolle darüber zu erlangen. (Bechis 2020, 120–21) Ähnlich wie europäische und andere westliche Staaten russische Versuche der Einflussnahme als Gefahr sehen, sieht das russische Regime die westliche „soft power“ als Bedrohung für den russischen Staat, die russischen Sicherheitsinteressen und die eigene Souveränität. Um der Bedrohung durch die „soft power“ zu begegnen, sieht man sich gezwungen, FIMI-Methoden permanent einzusetzen. (Fridman 2024)

Russland ist der Hauptakteur bei FIMI-Vorfällen in Europa und setzt FIMI-Kampagnen noch intensiver ein als China. Insbesondere die osteuropäischen Staaten sind massiven Einflussversuchen ausgesetzt. In Ländern mit russischsprachigen Minderheiten werden die

FIMI-Inhalte zudem in der russischen Sprache verbreitet, um somit die Spaltung der Gesellschaften voranzutreiben. Ein Land, welches in den letzten Jahren besonders stark in den Fokus russischer FIMI-Kampagnen geraten ist, ist die Ukraine. (Prysiazhniuk 2025) Seit dem Beginn des „Euromaidan“ im November 2013 nutzt Russland sämtliche verfügbaren FIMI-Werkzeuge, um die eigenen nationalen Ziele durzusetzen und die Souveränität der Ukraine zu untergraben. (EEAS 2023) Der seit 2022 jährlich erscheinende FIMI-Bericht des EEAS aus dem Jahr 2025 demonstriert, dass im Jahr 2024 die Ukraine erneut jenes Land gewesen ist, welches am meisten von den registrierten FIMI-Vorfällen betroffen gewesen ist. 257 Vorfälle sind 2024 in der Ukraine registriert worden, dies entspricht in etwa der Hälfte aller bekannten und vom EEAS dokumentierten Vorfälle. (EEAS 2025) Da nicht alle FIMI-Vorfälle vom EEAS erkannt und registriert worden sind und nicht jeder FIMI-Vorfall eindeutig einem Land zugeordnet werden kann, kann davon ausgegangen werden, dass die tatsächliche Anzahl an FIMI-Vorfällen noch höher ist.

Mit seinen FIMI-Kampagnen verfolgt Russland in Europa mehrere unterschiedliche strategische Ziele. Diese fokussieren sich zumeist darauf, Vorteile im Ukraine-Konflikt zu erlangen und den Zusammenhalt zwischen den europäischen Staaten zu untergraben. Das erste Ziel Russlands ist es, die Ukraine in der EU und in der internationalen Staatengemeinschaft zu diffamieren und zu diskreditieren. Damit möchte man erreichen, dass die internationalen Solidaritätsbekundungen sowie die humanitären, wirtschaftlichen und militärischen Unterstützungen an die Ukraine reduziert und beendet werden, beziehungsweise, dass es bereits initial keinen ausreichenden politischen Willen gibt, die Ukraine signifikant zu unterstützen. Dazu versucht man einzelne Bevölkerungsgruppen in den einzelnen Staaten so zu beeinflussen, dass deren Meinung über die Ukraine negativ ist. In weiterer Folge verändern diese beeinflussten Bevölkerungsgruppen die innenpolitischen Debatten und können somit ihre jeweiligen Regierungen dazu bewegen, Unterstützungsleistungen einzustellen. Ein hierfür häufig verwendetes Narrativ ist, dass die ukrainische Regierung sowie die ukrainischen Eliten korrupt seien und, dass daher Sachleistungen und Finanzhilfen aus dem Ausland nicht den Ukrainern oder dem ukrainischen Militär zu Nutze kommen, sondern zu den Oligarchen fließen. (EEAS 2023, 9) Russland zielt des Weiteren auch darauf ab, russlandfreundliche Politiker und Parteien durch das Schädigen ihrer

politischen Gegner zu unterstützen. Auf diese Weise schafft sich Russland ein wohlgesinnteres internationales Umfeld. Dies ist insbesondere im Zusammenhang mit den Entscheidungsmechanismen innerhalb der EU relevant. (Benkler, Farris, u. a. 2018) Bereits eine einzelne russlandfreundliche Regierung kann Beschlüsse, für die im Europäischen Rat Einstimmigkeit benötigt wird, blockieren oder verzögern. Für Russland ist insbesondere die GASP, zu der auch die Sanktionspakete gegen Russland gehören, relevant. So ist zum Beispiel das sechste Sanktionspaket zunächst von Ungarn blockiert worden. Dieses Veto wurde im Gegenzug für Zugeständnisse in anderen Bereichen wieder aufgegeben. (Müller und Slominski 2024, 113) Sollte eine russlandfreundliche Regierung durch die Unterstützung von FIMI-Kampagnen in einem EU-Mitglied die Regierungsverantwortung übernehmen, könnte diese Regierung sämtliche EU-Sanktionspakete sowie die europäische Verteidigungspolitik gegenüber Russland durch die Möglichkeit eines Vetos in Gefahr bringen.

Ein weiteres strategisches Ziel von Seiten Russlands ist es, in der Wahrnehmung der Weltöffentlichkeit nicht als kriegerischer Aggressor, sondern vielmehr als Verteidiger gegen die Hegemonialpolitik der USA und die Ausbreitung der NATO wahrgenommen zu werden. Wenn Russland in den Augen der Weltöffentlichkeit als Verteidiger beziehungsweise berechtigter Angreifer dar steht, kann man die Staatengemeinschaft in weiterer Folge davon überzeugen, Russland für sein völkerrechtswidriges Verhalten nicht wirtschaftlich oder politisch zu sanktionieren. Sehr dienlich und wirksam zum Erreichen dieses Ziels ist hierbei das Narrativ, dass der Westen Russland den Konflikt mit der Ukraine durch die NATO-Osterweiterung sowie die EU-Erweiterungen 2004 und 2007 regelrecht aufgezwungen habe. (EEAS 2023, 9) Ein weiteres zur internationalen Legitimierung des Kriegs verbreitetes FIMI-Narrativ ist, dass die Ukraine im Grunde genommen kein eigener Staat sei und, dass das ukrainische Volk ein Teil des russischen Volkes sei. Dies wird verstärkt durch die Falschbehauptung, dass die Ukraine systematisch die russische Minderheit im eigenen Land unterdrücke, wodurch Russland gezwungen gewesen sei zu deren Schutz zu intervenieren. (EEAS 2023) Zusätzlich wird durch FIMI-Kampagnen auch versucht, sowohl die ukrainische Zivilbevölkerung als auch die ukrainischen Militärangehörigen zu demoralisieren, um somit den Widerstand der Ukraine zu reduzieren und vermehrte Erfolge an der Front zu erreichen. Auf diese Weise soll der Krieg schneller gewonnen werden. (EEAS 2025; Prysiazhniuk 2025) Obwohl die russischen FIMI-

Operationen seit Beginn des „Euromaidan“ bis in die Gegenwart in ihrer Quantität und Qualität immer weiter gesteigert worden sind, sind die damit verfolgten Ziele im Grunde genommen dieselben geblieben. (EUvsDisinfo 2017) Seit der Vollinvasion im Februar 2022 ist es für Russland allerdings wichtiger geworden, die ukrainische Moral zu schwächen, um somit den Krieg rascher zu entscheiden. (Prysiazhniuk 2025)

Im FIMI-Bereich gilt Russland als sehr erfahrener und effektiv arbeitender Akteur, der global aktiv ist. Die Ursprünge der russischen Online-Informationsbeeinflussung und Medienmanipulation gehen auf die Gestaltung der russischen Medienlandschaft und der russischen Internetlandschaft zu Beginn der 2000er zurück. Zu Beginn der ersten Amtszeit von Vladimir Putin war die Verbreitung des Internets noch gering, sodass man sich die autoritäre Medienpolitik zunächst damit beschäftigte, die Massenmedien, also die großen Zeitungen und TV-Kanäle, auf einen regimetreuen Kurs zu bringen. Dies wurde erreicht, indem man Eigentümer der Medien änderte und Regimegegner in Exil zwang. In dieser frühen Zeit ist das Internet offen und von Restriktionen verschont geblieben. Bekler et al. (2018) vermuten, dass es im Internet zu keiner weitreichenden Zensur gekommen ist, weil die politischen Kosten der Zensur, den Nutzen für das Regime überstiegen hätten. Im Internet entwickelte sich daher eine politisierte Blog-Szene, in welcher auch Regime-kritische Stimmen zu hören waren. In eben dieser Blog-Szene wurden währen der Präsidentschaft von Dimitri Medvedev Regime-Sympathisanten aktiv, die sich aus Jugendgruppen zusammensetzten, welche das Aufkommen von Farbrevolutionen, wie sie unter anderem in Georgien oder der Ukraine stattgefunden haben, in Russland verhindern sollen. Beginnend mit Vladimir Putins Rückkehr in das Präsidentenamt 2012 wurden in Russland auch zunehmend die Medienfreiheit in Online-Blogs, durch veränderte Eigentümerstrukturen, gesetzlichen Druck und andere Mittel, eingeschränkt. In diese Zeit fällt auch die Geburtsstunde der ersten kommerziellen und professionellen Troll-Fabriken, die das Fundament für die späteren russischen Desinformationskampagnen wurden. Als eine solche Troll-Fabrik wurde 2013 die „Internet Research Agency“ (IRA) durch russische Investigativ-Journalisten bekannt. Die IRA stellt bezahlte Personen an, um den Online-Diskurs zu beeinflussen und zu manipulieren. Sie ist im Jahr 2018 im Rahmen der Ermittlungen zur russischen Einflussnahme auf die US-Präsidentschaftswahl 2016 vom FBI-Sonderermittler Robert Mueller angeklagt worden.

(Benkler, Farris, u. a. 2018, 236–39) In dem Bericht von Robert Mueller wird die IRA als eine russische Organisation beschrieben, die von Yevgeny Prigozhin aufgebaut und finanziert worden ist. (Bechis 2020, 126) Inzwischen sind neben der IRA auch die staatlichen Medien, Online-Portale, etablierte private Medienhäuser und die verschiedenen russischen Geheimdienste in die FIMI-Maschinerie involviert. Insbesondere die Geheimdienste nutzen dabei auch staatsnahe Gruppen, die so genannten Proxies. Diese haben für Russland den Vorteil, dass sie die Attribuierung von FIMI-Vorfällen erschweren und, dass der Staat seine Beteiligung an deren Aktionen abstreiten kann. (EEAS 2023, 28–29) In der nachstehenden Grafik werden bekannte russische FIMI-Akteure sowie deren Zugehörigkeit, basierend auf Erkenntnissen des EEAS, dargestellt.

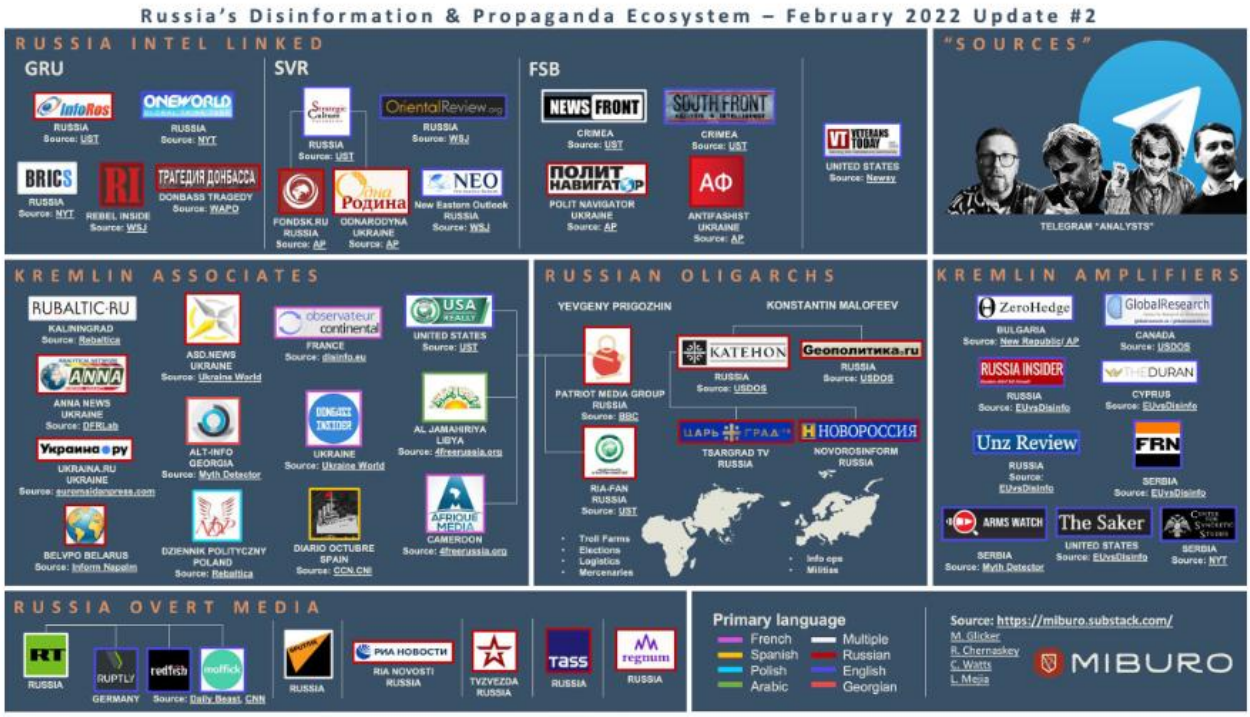

Abbildung 3: EEAS (2023) The russian FIMI ecosystem

5.2 China als Bedrohungsakteur

Die Verwendung hybrider Mittel durch die chinesische kommunistische Partei hat eine lange Historie. Dies reicht von der Verwendung wirtschaftlichen Drucks, wie zum Beispiel im Rahmen der Belt and Road initiative, bis hin zu Spionage und Cyber-Angriffen. (Hjortdal 2011) Seit 2019 ist auch nachgewiesen, dass China FIMI-Werkzeuge zur Durchsetzung strategischer Ziele

anwendet. So gelang dem EEAS die Attribuierung von Desinformationsnetzwerken auf Twitter und Facebook. Inzwischen ist auch bekannt, dass die chinesische Regierung bezahlte Influencer und andere einflussreiche Personen im Ausland nutzt, um Kritik am eigenen Regime entgegenzutreten, die Narrative rund um die Umerziehungslager in Xinjiang zu beeinflussen und generell die öffentliche Meinung über China zu verbessern. (EEAS 2023)

In den vergangenen Jahren haben sich chinesischen Desinformation-Versuche hauptsächlich im Zusammenhang mit den Demokratie-Protesten in Hong-Kong 2019 und 2020, der Verbreitung und dem Ausbruch der Covid-19 Pandemie im chinesischen Wuhan sowie der taiwanesischen Parlaments- und Präsidentschaftswahl 2020 ereignet. (Hung und Hung 2022) Ebenso wird mittels FIMI-Kampagnen versucht, Einfluss auf demokratische Wahlen in liberalen Nachbarländern wie Australien und Südkorea zu nehmen. (Girardi u. a. 2025) Den FIMI-Kampagnen gegen Taiwan liegen die chinesischen Bestrebungen zugrunde, dass man Taiwan, welches man in China nur als abtrünnige Provinz aber nicht als eigenständigen Staat betrachtet, wieder mit dem Festland vereinigen möchte. Dementsprechend bemüht sich China mittels Desinformation beziehungsweise FIMI, die Bürger Taiwans davon zu überzeugen, dass die Wiedervereinigung ihre beste und einzige Option ist. Die Beeinflussung äußert sich dadurch, dass regelmäßig Narrative und Geschichten verbreitet werden, dass Taiwan allein wirtschaftlich nicht überlebensfähig sei oder, dass die taiwanesische Regierung nicht in der Lage sei, die eigene Bevölkerung vor diversen Bedrohungen zu beschützen. Die chinesische Regierung greift hierfür auf verschiedene Methoden zurück. Diese sind zum Beispiel der Erwerb von taiwanesischen Medienunternehmen oder reichweitenstarker Social-Media-Kanäle durch chinesische Unternehmen oder Parteimitglieder, um über diese glaubhafte Desinformation zu verbreiten. Insbesondere die Online-Plattform YouTube ist ein beliebtes Vehikel zur Verbreitung von Desinformation geworden, da auf dieser Plattform im Vergleich zu anderen Plattformen weniger Inhalte entfernt werden und somit Desinformation länger bestehen kann. (Zhang 2020)

Eine prominente chinesische FIMI-Kampagne, mit der versucht worden ist, den öffentlichen Diskurs in Europa, den USA und Kanada zu beeinflussen, ist die von 2019 bis 2022 aktive „Dragonbridge-Kampagne“. Diese ist auch unter dem Namen „Spamouflage“ bekannt geworden. Bei dieser FIMI-Operation hat mutmaßlich die, im chinesischen Ministerium für

öffentliche Sicherheit angesiedelte, „912 Special Project Working Group“ Social-Media-Accounts erstellt, die massenhaft Bilder und Videos von chinesischen Landschaften gezeigt haben. In diese Ansammlungen von Landschaftsbildern sind einzelne Posts und Videos gemischt worden, die unter anderem die Demokratiebewegung in Hong-Kong diffamieren oder die Kritik an den Umerziehungslagern in Xinjiang zurückweisen und als westliche Propaganda abtun. Des Weiteren hat man im Jahr 2022 mit dieser Methode versucht, sowohl im Zusammenhang mit den US-Zwischenwahlen als auch im Rahmen der Sprengung der „Nordstream 2 Pipeline“, Einfluss auf die öffentliche Meinung in den USA und Europa zu nehmen. Laut eigener Auskunft hat Google im Jahr 2022 50.000 Konten gesperrt, die im Verdacht gewesen sind, Teil der „Dragonbridge-Kampagne“ zu sein. Obwohl eine sehr große Zahl an Accounts für diese FIMI-Kampagne genutzt worden ist, gilt diese Kampagne nur als wenig erfolgreich, da die einzelnen Posts und Videos nur sehr wenige Aufrufe generieren konnten. In den meisten Fällen haben diese weniger als 100 Aufrufe. Die geringe Wirksamkeit der FIMI-Kampagne wird auf fehlende kulturelle Adaption sowie unkoordinierte Techniken zurückgeführt. (O’Sullivan u. a. 2023) Der geringe Erfolg der „Dragonbridge-Kampagne“ sollte von den europäischen Staaten als Warnung verstanden werden, dass China willens ist auf hybride Mittel zurückzugreifen und vermutlich auch in Zukunft erneut Versuche unternehmen wird, die öffentliche Meinung im Ausland zu beeinflussen. China kann aus den gemachten Fehlern lernen und mit einer besser gestalteten FIMI-Kampagne und klaren strategischen Zielen Erfolge erzielen.

Zur Steigerung der Reichweite von FIMI-Kampagnen verfügt die chinesische Regierung über großen Einfluss auf die bei Jugendlichen populäre und zum chinesischen Unternehmen Bytedance gehörende Online-Plattform TikTok. Durch das chinesische „National Intelligence Law“ ist die chinesische Regierung stets dazu berechtigt, Zugriff und Einfluss auf die Moderationsrichtlinien der Plattform, die Nutzerdaten und die Entscheidungslogarithmen zu nehmen. Durch Manipulationen des TikTok-Algorithmus kann man gezielt pro-chinesische Narrative verbreiten und kritische sowie anti-chinesische Meinungen systematisch unterdrücken. Der EEAS geht in seinem FIMI-Bericht 2024 davon aus, dass China in Zukunft seinen Einfluss auf Plattformen wie TikTok nutzen wird, um das eigene FIMI-Arsenal zu

verstärken. Aus diesem EEAS-Bericht geht ebenso hervor, dass China auch staatliche kontrollierte klassische Medien vermehrt für FIMI-Kampagnen nutzen wird. (EEAS 2025)

6 Die Strategien zur Abwehr von FIMI-Kampagnen

Nachdem im vorhergehenden Kapitel, die Bedrohungsakteure Russland und China sowie deren Vorgehen und Strategien beschrieben worden sind, widmet sich dieses Kapitel den verschiedenen Ansätzen, mit denen man FIMI-Kampagnen abwehren beziehungsweise deren Wirksamkeit und Gefahr mindern kann. Die verschiedenen Ansätze sind im ersten FIMI-Bericht des EEAS in vier übergeordnete Kategorien unterteilet worden. Diese sind: Detektion, Reaktion in Form von Restriktionen oder Richtigstellungen, Prävention und internationale Kooperation. Jede dieser vier verschiedenen Abwehrformen erfüllt eine andere Funktion und erfordert daher auch unterschiedliche mitwirkende Akteure. (EEAS 2023)

Im folgenden Kapitel wird zunächst das vom EEAS verwendete Framework zur Erkennung, Einordnung und Analyse von FIMI-Vorfällen beschrieben. Anschließend werden verschiedene Methoden, die dem Unterbinden von FIMI-Kampagnen dienen und die Bevölkerung schützen sollen, aufgezählt. Dabei werden Methoden beschrieben, mit denen es möglich ist, den Angreifer daran zu hindern Desinformation zu verbreiten oder eine Vielzahl an Menschen zu erreichen. Im nachfolgenden Abschnitt werden dann verschiedenen Vorgehensweisen erklärt, mit denen es möglich ist, die Resilienz der Menschen zu steigern. Abschließend werden noch Strategien, die auf internationaler Kooperation basieren, erklärt.

6.1 Die DISARM-Methode

Zur Verteidigung gegen FIMI gibt es verschiedene „Frameworks“. Eines von diesen ist die vom EEAS entwickelte DISARM-Methode. DISARM steht in diesem Fall für „Disinformation Analysis and Risk Management“ und ist ein offenes Framework zur Analyse und Dokumentation von FIMI-Operationen sowie deren Techniken, Praktiken und Prozessen. Inzwischen wird auch von der NATO und der EU daran gearbeitet, das DISARM Framework zu einer internationalen Norm im Bereich der FIMI-Verteidigung zu machen. Dieses Framework besteht aus dem ABCDE-Modell, zur Analyse und Dokumentation von FIMI-Vorfällen, und der so genannten Kill-Chain zum Verhindern und Beenden einzelner FIMI-Vorfälle. (EEAS 2023) Die Kill-Chain basiert auf

einem erprobten Ansatz aus dem Bereich der Cyber-Sicherheit. Hierbei geht man davon aus, dass jede FIMI-Kampagne, ähnlich wie ein Cyber-Angriff, aus mehreren aufeinander aufbauenden Schritten besteht. FIMI-Kampagnen sind also mehrstufige Prozesse, die aus den Schritten Planung, Produktion von Inhalten, Verbreitung, Verstärkung der Inhalte und Analyse des Erfolgs bestehen. Jeder dieser Schritte wiederum besteht aus verschiedenen Taktiken, Techniken und Prozessen. Zur Verbreitung kann der Angreifer zum Beispiel Bot-Netzwerke in sozialen Medien, Kopien von Webseiten renommierter Zeitungen oder gekaufte Akteure im Zielland verwenden. Die Methode der Kill-Chain geht nun davon aus, dass man den gesamten FIMI-Prozess stoppen kann, wenn man es schafft, eines der Glieder auszuschalten. Wenn man also zum Beispiel den Schritt der Produktion ausschaltet oder dem Angreifer die benötigte Methode zur Verbreitung vorenthält, kann man den Prozess als gesamtes stoppen und somit den FIMI-Vorfall beenden. (EEAS 2023)

Das ABCED-Modell ist von James Pamment entwickelt worden und wir momentan vom EEAS zur Klassifizierung und Einordnung von FIMI-Vorfällen verwendet. Beim ABCDE-Modell wird ein einzelner FIMI-Vorfall in die fünf Kernelemente, „Actor, Behaviour, Content, Degree und Effect“ unterteilt. In der Kategorie „Actor“ wird der Urheber eines FIMI-Vorfalls identifiziert. Die Kategorie „Behaviour“ beschreibt die verwendeten Methoden, Prozesse und Taktiken und die Kategorie „Content“ die verwendeten Narrative der FIMI-Vorfälle. „Degree“ und „Effect“ beschreiben schließlich die Verbreitung eines FIMI-Vorfalls sowie dessen Wirkung. (Pamment 2020a) Damit das DISARM-Framework international und bereichsübergreifend verwendet werden kann, werden die dort gespeicherten Daten mit dem STIX2 Sprach- und Strukturformat gespeichert. Dieses Datenformat wurde für die Erkennung von Cyber-Bedrohungen entwickelt und verfeinert. Ein weiterer Vorteil der einheitlichen Verwendung von STIX2 ist, dass somit die Erkennung und Kategorisierung von FIMI-Vorfällen automatisiert werde könnte, wodurch die FIMI-Verteidiger auf einzelne Vorfälle schneller agieren könnte und somit der Vorteil der Angreifenden verringert werden könnte. (European Union Agency for Cybersecurity 2022) Die nachstehende Grafik veranschaulicht noch einmal das Funktionieren der ABCDE-Methode und stellt einige Beispiele dar.

Table 4 The ABCDE framework for FIMI analysis according to James Pamment.

Actor	*What kinds of actors are involved? This question can help establish, for example, whether the case involves a foreign state actor.*
Behaviour	*What activities are exhibited? This inquiry can help establish, for instance, evidence of coordination and intent.*
Content	*What kinds of content are being created and distributed? This line of questioning can help establish, for example, whether the information being deployed is deceptive.*
Degree	*What is the distribution of the content? Which audiences were targeted and reached?*
Effect	*What is the overall impact of the case and whom does it affect? This question can help establish the actual harms and severity of the case.*

Abbildung 4: James Pamment (2020) The EU's Role in Fighting Disinformation: Crafting A Disinformation Framework

Da ständig neue Techniken, Taktiken und Prozesse zur Verbreitung von FIMI entwickelt werden, muss auch das DISARM Framework stetig verbessert und an die sich verändernden Bedrohungen angepasst werden. So hat in den letzten Jahren beispielsweise die Notwendigkeit bestanden, auf das Aufkommen von KI-generierten Inhalten entsprechend zu reagieren. Der EEAS schlägt für die Verbesserung der FIMI-Abwehr vor, dass das Sammeln von Daten standardisiert abläuft. Des Weiteren ist das DISARM Framework trotz seiner Struktur auch limitiert. Es ist stark auf technisch analysierbare und öffentlich zugängliche sowie sichtbare Daten angewiesen. FIMI-Operationen, die auf verdeckte Akteure wie zum Beispiel staatliche Proxys zurückgreifen, lassen sich ebenso wie Einflussoperationen, die in diplomatischen Kanälen ablaufen, nur schwer durch das Framework erfassen. (EEAS 2023)

6.2 Inhaltsmoderation und Entfernen von FIMI-Vorfällen

Das Löschen und Entfernen von Desinformation ist ein elementarer Bestandteil in der Verteidigung gegen FIMI. Die Logik der Inhaltsmoderation ist leicht nachzuvollziehen: FIMI-Vorfälle, die keine oder nur wenige Menschen erreichen, können keine Wirkung beziehungsweise nur geringe Wirkung entfalten. Man entfernt also FIMI-Inhalte von Plattformen, um somit sicherzustellen, dass diese nicht verbreitet werden. Die Strategie des Entfernens ist allerdings auch mit zahlreichen technischen, rechtlichen, ethischen, politischen, gesellschaftlichen und zum Teil auch wirtschaftlichen Problemen verbunden. Staaten, Behörden und private Unternehmen sind dazu angehalten, bei der Inhaltsmoderation

besondere Vorsicht walten zu lassen, damit durch das Entfernen von Inhalten die Rechte auf Meinungs- und Pressefreiheit nicht übermäßig eingeschränkt werden. (Bridgman u. a. 2024)

Wie bereits zuvor beschrieben sind Soziale-Medien ein häufig genutztes Werkzeug zur Verbreitung von FIMI. In der Regel sind die Betreiber von Plattformen für das Entfernen von Inhalten verantwortlich und haben das Recht zu entscheiden welche Inhalte auf den jeweiligen Plattformen verbreitet werden können. Plattformen sollten im Idealfall über klare und transparente Richtlinien verfügen, anhand derer sie beurteilen, welche Inhalte entfernt werden. Die großen Mengen an Posts und Inhalten auf den verschiedenen Plattformen bedingt, dass Algorithmen bei der Inhaltsmoderation eingesetzt werden müssen, da Menschen diese Menge ohne Unterstützung nicht mehr bearbeiten können. Diese Algorithmen sollten ihre Entscheidungen ebenso aufgrund transparenter Richtlinien treffen. Bei der Gestaltung der Algorithmen sollte des Weiteren darauf geachtet werden, dass diese keine politischen Vorurteile haben. Sie dürfen also nicht aktiv in die Meinungsbildung eingreifen, indem sie gewisse Meinungen unterdrücken. (Gonçalves u. a. 2023, 2597) Desinformation und FIMI sollte unabhängig von der politischen Zuordnung beurteilt werden, da ansonsten das Vertrauen in die Inhaltsmoderation verloren geht. Aufgrund des so genannte Streisand-Effektes ist es bei der Inhaltsmoderation sogar möglich, dass die Brisanz von Inhalten durch das Entfernen erhöht wird und somit die Aufmerksamkeit der Menschen und die Glaubhaftigkeit des entfernten Inhalts steigt. In so einem Fall kann die Inhaltsmoderation das Gegenteil der erwünschten Wirkung erzielen und die Wirksamkeit von FIMI sogar noch weiter steigern. (Martin und Jansen 2015)

Inhaltsmoderation ist für die Betreiber großer Plattformen ein sehr kostenintensives und personalintensives Unterfangen, daher neigen diese häufig dazu, ihre Bemühungen auf ein Minimum zu beschränken. Regierungen können dem entgegenwirken, indem sie Plattformen zu strikter Inhaltsmoderation verpflichten und bei Nicht-Einhaltung strenge Strafen verhängen. Staaten und Regierungen sind allerdings aufgrund möglicher Einschränkungen der Meinungs- und Redefreiheit sehr zurückhaltend, verpflichtende und konsequente Inhaltsmoderation einzuführen. (Kozyreva u. a. 2023)

6.3 Fact-Checking, Strategische Kommunikation und Korrektursysteme

Neben dem Unterbinden der Verbreitung von Desinformation gibt es auch noch eine andere Strategie, um die Wirksamkeit von FIMI-Kampagnen zu reduzieren. Narrative Gegenstrategien und proaktive strategische Kommunikation zielen darauf ab, Fehlinformationen vorzubeugen und alternative Sichtweisen anzubieten. (Humprecht u. a. 2020) Mit dieser Strategie nimmt man FIMI-Kampagnen durch den Fokus auf wahre und überprüfbare Informationen ihre Wirkung. Fact-Checking nimmt im Kampf gegen FIMI eine zentrale Rolle ein, da sich damit falsche Informationen richtigstellen und überprüfen lassen. Die Wirkung von Fact-Checking kann allerdings eingeschränkt sein, weil Menschen sich eher von Informationen überzeugen lassen, die ihren eigenen Weltanschauungen beziehungsweise ihren bereits bestehenden Meinungen entsprechen. Dieses Phänomen nennt man entweder „confirmation bias“ oder „motivated reasoning“. Dieses Phänomen führt dazu, dass selbst der sorgfältigsten Richtigstellung nicht geglaubt wird. Insbesondere politisch polarisierte Personen und Personen, die anfällig für populistische Rhetorik sind, lassen sich durch Fact-Checking nur schwer überzeugen. (Humprecht u. a. 2020, 5–6)

Eine Art des Fact-Checkings, mit der sich die Verbreitung von FIMI wirksam einbremsen lässt, ist die Echtzeitüberprüfung auf Sozialen-Medien und Nachrichtenplattformen. Irreführende Information und FIMI werden hierbei möglichst früh durch das Einblenden von Bannern mit Korrekturen, richtigstellender Kommentare oder anderer visueller Warnhinweise als falsch gekennzeichnet. Somit werden die Nutzer der Sozialen-Medien und der Nachrichtenplattformen direkt über den Wahrheitsgehalt der Inhalte informiert. Solche Überprüfungen und Korrekturen sind allerdings nur dann effektiv, wenn sie transparent und erklärend sind. Eine effektive Echtzeitüberprüfung informiert sowohl über die Quelle des Faktenchecks als auch über die Gründe, weshalb der entsprechende Inhalt als Desinformation oder FIMI eingestuft worden ist. (Bayer u. a. 2019, 114–15) In den letzten Jahren sind von einigen Online-Plattformen solche Systeme eingeführt worden und auch einige etablierte Medien setzen inzwischen auf Echtzeitüberprüfungen. Auf der Plattform X, vormals Twitter, können andere Nutzer in Form von „Community Notes“ weitere Informationen zu einem irreführenden Post hinzufügen. In diesen „Community Notes“ werden unter anderem auch Verweise und Links zu Wikipedia oder anderen Medien angeführt. (Drolsbach u. a. 2024)

Ob Fakten-Checks tatsächlich wirksam sind, ist umstritten. Eine Untersuchung von Twitter-Datensätzen durch Shin und Thorson (2017) hat gezeigt, dass Menschen in erster Linie Fakten-Checks teilen und weiterleiten, wenn der Kandidat der eigenen Partei oder die eigene politische Ideologie durch den Fakten-Check unterstützt werden oder, wenn dem politischen Gegner dadurch geschadet wird. Die Autoren bezeichnen dieses Phänomen als „selective sharing" und meinen damit, dass Nutzer lediglich für Fakten-Checks zugänglich sind, wenn diese der eigenen politischen Überzeugung entsprechen. (Shin und Thorson 2017) Eine empirische Studie von Vargo et al. bestätigt, dass der Effekt von Fakten-Checks auf das öffentliche Narrative nur sehr gering ist und Menschen es bevorzugen an ihren bestehenden Überzeugungen festzuhalten. (Vargo u. a. 2018)

6.4 Präventive Strategien, Medienlandschaften und „Digital Literacy"

Die präventiven Strategien und Methoden verfolgen das übergeordnete Ziel, die eigenen Bevölkerung sowie die demokratischen Institutionen gegenüber FIMI und Desinformation resilient zu machen. Dabei wird die zugrundeliegende Logik verfolgt, dass Menschen, die FIMI-Vorfälle und desinformierende Nachrichten als solche erkennen, nicht von FIMI und Desinformation in ihrer Meinungsbildung und ihren Entscheidungen beeinflusst werden können. Es existieren verschiedene Faktoren, die sowohl zu einer Erhöhung als auch zu einer Reduktion der gesellschaftlichen Resilienz beitragen können.

Faktoren, die die Resilienz einer Bevölkerung in einzelnen Ländern schwächen oder stärken können, kann man nach Humprecht et al (2020) in drei verschiedene übergeordnete Kategorien aufteilen. In die erste Kategorie fallen die Faktoren des politischen Umfelds. Dazu gehören die Polarisierung der Gesellschaft sowie populistische „Wir gegen Sie"- Rhetorik. Eine polarisierte Gesellschaft, wie sie vor allem in Ländern mit Mehrheitswahlrecht existiert, schwächt die Resilienz gegen Desinformation, da Menschen dazu neigen, wahre Informationen, die negativ über die eigene politische Überzeugung berichten, zu ignorieren. Desinformation, die ein negatives Narrative über die andere politische Seite erzählt, wird hingegen eher weiterverbreitet. Ein hoher Grad an politischer Polarisierung und eine dementsprechende Emotionalisierung führen dazu, dass Information nicht mehr rational beurteilt wird sondern emotional. Populistische Rhetorik hingegen hat negative Effekte auf die

Resilienz, da damit ein Mistrauen gegen Experten, etablierte Medien und die Eliten geschürt wird, weil diese Gruppe angeblich gegen die Interessen der Bevölkerung arbeiten. Wenn solches Mistrauen existiert, ist die Widerlegung von Desinformation und die Verbreitung von wahrer Information erschwert. (Humprecht u. a. 2020, 8–11) Die zweite Kategorie, der Resilienz schwächenden Faktoren, ist jene der Medienlandschaft. Hierbei haben die Faktoren geringes Vertrauen in etablierte Medien, schwache öffentlich-rechtliche Medien und eine stark fragmentierte beziehungsweise wenig überlappenden Medienlandschaft negative Effekte auf die Widerstandsfähigkeit der Bevölkerung. Geringes Vertrauen in etablierte Medien führt dazu, dass Menschen anfälliger für Desinformation und FIMI sind, weil sie eher auf Online-Medien oder alternative Medien zugreifen, die in der Regel weniger Wert auf journalistische Standards und faktenbasierte Berichterstattung legen. Des Weiteren führt Misstrauen gegenüber etablierten Medien zu einer geringeren Auseinandersetzung mit verschiedenen Quellen und zu deren kritischer Reflexion. In Ländern mit stark ausgeprägten öffentlich-rechtlichen Medien verfügt die Bevölkerung über verbesserten Zugang zu qualitativ hochwertigen Nachrichten. Dies führt in weitere Folge dazu, dass private Medienunternehmen ihre Qualität steigern müssen, um sich am Informationsmarkt zu behaupten. Somit entsteht ein Qualitätswettbewerb, der generell das Wissen innerhalb der Bevölkerung steigert. (Humprecht u. a. 2020, 11–12) Damit die Medien vermehrt zur Resilienzsteigerung beitragen können, ist eine professionelle und bestenfalls entpolitisierte beziehungsweise unparteiische Medienlandschaft notwendig. In hochpolitisierten Medienlandschaften, in denen sich Medien politischen Parteien eindeutig zuordnen lassen, agieren Medien weniger als Fakten-Checker, sondern vermehrt als Vehikel zur Bestätigung bereits bestehender Meinungen. Eine hoch polarisierte Medienlandschaft kann somit zur Verbreitung von Desinformation und FIMI beitragen. (Benkler, Faris, u. a. 2018) Als dritte Kategorie der Resilienz beeinflussenden Faktoren benennen Humprecht, Esser und Van Aelst (2020) die Faktoren des wirtschaftlichen Umfelds. In diese Kategorie fallen die Faktoren des nationalen Online-Werbemarktes und die Nutzung von Sozialen-Medien. Das Wirtschaftsmodell von großen Online-Plattformen wie Facebook und Youtube basiert auf dem Anzeigen von Werbung. Nutzer, die Desinformation und FIMI verbreiten wollen, können dadurch mit ihren unrichtigen Inhalten Geld verdienen. Dies führt in weiterer Folge dazu, dass insbesondere große Online-Märkte, auf denen viel Werbung inseriert wird und somit die Ersteller der Inhalte viel Geld verdienen können, für

Desinformation interessanter sind als kleine Online-Märkte. Daher ist auch vermehrt Desinformation auf großen Online-Märkten zu finden. Ein weiterer Faktor, der die Resilienz eine Bevölkerung gegen Desinformation negativ beeinflusst ist die Intensität der Nutzung von Sozialen-Medien. Diese sind ein Brutkasten für Desinformation und deren Verbreitung, weil Nutzer diese eher als Quelle der Unterhaltung betrachten und nicht als Informationsquelle. Somit sind Nutzer gegenüber falschen Informationen weniger achtsam und verbreiten selbst auch eher Desinformation. Gesellschaften mit einer vielen Nutzern von Sozialen-Medien sind Desinformation daher vermehrt ausgesetzt und somit auch weniger resilient. (Humprecht u. a. 2020)

Vor dem Hintergrund dieser Vielzahl an Resilienz schwächenden Faktoren stellt sich nun die Frage, mit welchen politischen, gesellschaftlichen sowie bildungspolitischen Maßnahmen die Resilienz von Gesellschaften erhöht werden kann. Bayer et al. (2019) schreiben hierzu, dass es ein elementarer Bestandteil präventiver Strategien sein sollte, die Bürger gut zu informierten und zu kritischen Denkern zu formen. Hierbei ist es wichtig, ein Bewusstsein für die Bedrohungen durch Desinformation und FIMI im Internet im Sinne der „digital literacy“ zu schaffen. Man muss der Bevölkerung bewusst machen, dass insbesondere im Rahmen von Wahlen und Wahlkämpfen der Online für die Verbreitung von Desinformation genutzt wird. Für die Bildung einer ausgeprägten „media literacy“ bietet sich in der Regel das Schulsystem an. Hier können bereits in jungem Alter Wissen und Kompetenzen vermittelt werden, die ein Leben lang bestehen. Da man mit der Aufklärung im Schulunterricht allerdings nur die jungen Bevölkerungsschichten erreichen kann, sollten Staaten auch Strategien und Prozesse entwickeln, um ältere Menschen auf die Probleme mit Desinformation und ausländischer Beeinflussung aufmerksam zu machen. Diese sind ebenso anfällig für Beeinflussung und durch ihre Lebenserfahrung nicht vor Gefahren und Einflussnahmen geschützt. (Bayer u. a. 2019) Das deutsche Bundesamt für Verfassungsschutz schreibt hierzu, dass man Bürger dazu befähigen soll, Desinformation kritisch zu hinterfragen und FIMI selbstständig zu erkennen. Ein Multistakeholder-Ansatz, der verschiedene Akteure einbezieht, ermöglicht koordinierte Bemühungen und den Austausch von Expertise. (Bundesamt für Verfassungsschutz 2023)

6.5 Die Attribuierung der Urheber und Sanktionen gegen Staaten

Ein zusätzlicher Schritt zur Verteidigung gegen FIMI-Kampagnen ist die Attribuierung des Angreifers. Hierbei versucht man einen FIMI-Vorfall einem Land, einer Organisation oder einer Einzelperson eindeutig zuzuordnen. Anhand cyber-forensischer Erkenntnisse kann man ähnlich wie bei einem Cyberangriff herausfinden, welche Personen oder Gruppen verantwortlich für die Verbreitung eines bestimmten FIMI-Vorfalls sind. (Banks 2019) Gegen diese Personen oder Gruppen können Staaten in weiterer Folge Sanktionen verhängen und, wenn möglich, auch Strafprozesse einleiten. Da sich die verantwortlichen Personen oft in Staaten wie Russland oder China aufhalten, ist es schwierig, diese juristisch zur Verantwortung zu ziehen. Das Verhängen von wirtschaftlichen oder politischen Sanktionen gegen Staaten , die FIMI betreiben, hingegen erhöht die potenziellen Kosten der Angreifer und kann diese somit davon abhalten, FIMI-Kampagnen zu betreiben. (Davituliani 2024) Da Staaten wie Russland, Iran oder Nordkorea bereits stark sanktioniert sind, ist es unwahrscheinlich, dass sich diese Staaten durch zusätzliche Sanktionen abschrecken lassen. Potentielle Sanktionen können allerdings dazu führen, dass andere Staaten von der Durchführung von FIMI-Kampagnen abgeschreckt werden.

7 Methodisches Vorgehen

Zur Beantwortung der Forschungsfrage: „Warum unterscheiden sich die Strategien und Verteidigungs-Policies europäischer Staaten gegen FIMI“ wird ein Policy-Vergleich verschiedener EU-Staaten durchgeführt. Da es sich bei FIMI-Bedrohungen um ein vergleichsweise neues Phänomen handelt, sind noch nicht von allen europäischen Staaten Gegenmaßnahmen ausgearbeitet oder umgesetzt worden. In einigen Staaten wird das Problem von Seiten der Politik nicht als solches wahr genommen, beziehungsweise gibt es in einigen Ländern von Seiten der Politik Unterstützung für FIMI, da Politiker zum Teil von ausländischer Beeinflussung profitieren können. (Janda u. a. 2017) Des Weiteren sind manche Länder wesentlich stärker im Fokus ausländischer FIMI-Kampagnen als andere, wodurch für diese Länder ein höherer Handlungsdruck entsteht. In dieser Masterarbeit werden vier Fälle ausgewählt. Bei diesen handelt es sich um Länder, die bereits erste Maßnahmen gegen FIMI erlassen haben. Da es das primäre Ziel dieser Arbeit ist, herauszufinden aus welchen Gründen

sich die Policies verschiedener Länder unterscheiden, wird bereits bei der Fallauswahl darauf geachtet, dass die ausgewählten Länder sich für unterschiedliche Wege der Problemlösung entschieden haben. Die ausgewählten Länder sind Deutschland, Frankreich, Schweden und Österreich.

7.1 Verwendete Methode

Zur Beantwortung der Forschungsfrage: „Welche Strategien und Policy-Maßnahmen implementieren ausgewählte europäische Länder zur Abwehr und Bekämpfung von FIMI-Kampagnen? Welche relevanten Unterschiede gibt es zwischen den verschiedenen Ländern und wie kann man eine mögliche Konvergenz der Strategien im Laufe der Zeit erklären?“ wird in dieser Arbeit eine vergleichende Fallstudienanalyse angestrebt. Diese erlaubt es die Unterschiede und Gemeinsamkeiten der Länder zu erkennen und macht es darüber hinaus möglich, ein tiefgreifendes Verständnis für die nationalen Strategien, politischen Gegebenheiten und die unterschiedlichen nationalen Situationen zu generieren. (Blatter und Haverland 2012, 37–40) Mit dieser Methodik soll sich ebenso eruieren lassen, wie europäische Koordinationsmechanismen eine Konvergenz der unterschiedlichen nationalen Strategien erklären können.

Das verwendete Forschungsdesign ist hierbei ein „Most similar systems design“ (MSSD). Das bedeutet, dass bei der Fallauswahl darauf geachtet wird, Länder mit möglichst ähnlichen Rahmenbedingungen zu wählen, sich aber dennoch unterscheiden. Ein MSSD, bei dem die Rahmenbedingungen der verschiedenen Länder ähnlich sind, erlaubt es innerhalb der homogenen Fallauswahl Faktoren für Unterschiede in der FIMI-Abwehr herauszufiltern. (Przeworski und Theune 1970) Zur Erstellung der Fallstudien werden qualitative Inhaltsanalysen der verschiedenen nationalen Sicherheitsstrategien und FIMI- beziehungsweise Desinformationsstrategien erstellt. Ebenso werden, wenn diese verfügbar sind, auch Dokumente zum Prozess der Strategieerstellung miteinbezogen. Die qualitative Inhaltsanalyse erlaubt es, den Sinn von Policy- und Gesetzesdokumenten strukturiert zu analysieren und dabei den jeweiligen Entstehungskontext zu inkludieren. Da die Entstehung von Policy-Veränderungen komplex und oft nicht formalisiert ist, erlaubt eine qualitative

Inhaltsanalyse von Policy-Dokumenten und Strategien die jeweiligen Zusammenhänge in ihrem historischen Kontext zu verstehen. (Mayring und Fenzl 2019)

Die Analyse stützt sich auf die in Kapitel 3 beschriebenen Theorien zur Policy-Veränderung und deren zentrale Mechanismen, wie Pfadabhängigkeit, „Coordinative Europeanisation“ und die OMK. Die Fallstudien zu den verschiedenen Ländern werden anschließend miteinander verglichen. Somit kann herausgefunden werden, welche Faktoren die jeweiligen Policy Veränderungen beeinflusst haben und welche nationalen Eigenschaften und externen Ereignisse eine Rolle bei der Entwicklung der Policies gespielt haben. Abschließend kann mit diesem methodischen Gerüst erklärt werden, ob sich die bestehenden Theorien zu Policy-Veränderungen sowie ihre Mechanismen auf die Entwicklung der FIMI-Abwehr und der nationalen Strategien anwenden lassen.

7.2 Fallauswahl

Wie zuvor beschrieben wird in dieser Arbeit ein „Most similar system design“ (MSSD) angewandt. Daher weisen die ausgewählten Fälle, Deutschland, Frankreich, Schweden und Österreich, eine hohe Zahl an Überschneidungen und Gemeinsamkeiten auf. Die ausgewählten Länder sind alle Mitglieder der EU, weisen alle eine intakte demokratische und rechtsstaatliche Grundordnung auf und verfügen im Bereich der FIMI-Bedrohung über eine annähernd vergleichbare sicherheitspolitische Problemwahrnehmung. Des Weiteren handelt es sich um Länder, mit einer hohen Pressefreiheit. So erreichen alle Länder im „Press Freedom Ranking“ aus dem Jahr 2024 entweder die Note Gut oder die Note Zufriedenstellend. Frankreich hat hierbei mit 76,62 Punkten von 100 möglichen Punkten den niedrigsten Wert und Schweden mit 88,13 Punkten den höchsten. (Reporters without borders 2025)

Neben diesen Gemeinsamkeiten unterscheiden sich die Länder allerdings in ihrer institutionellen Beschaffenheit, ihrer Historie mit FIMI-Ereignissen, in den jeweiligen nationalen behördlichen Zuständigkeiten sowie in der Reichweite und Zielsetzung ihrer FIMI-Abwehrmaßnahmen. Nach dem NATO-Beitritt Schwedens im Jahr 2024 ist Österreich das einzige ausgewählte Land, welches kein Mitglied des Verteidigungsbündnisses ist. Allerdings hat Österreich im Rahmen der „NATO Partnership for Peace“ (PfP) die Möglichkeit an NATO-Programmen zur Kapazitäts- und Resilienzbildung teilzunehmen und ist somit nicht isoliert von

den Entwicklungen und den Erfahrungsgewinnen innerhalb der NATO. Österreich wurde aber bewusst als Fall ausgewählt, damit beobachtet werden kann, ob und welche Unterschiede sich durch die fehlende Bündnismitgliedschaft sowie durch die immerwährende Neutralität ergeben.

Die ausgewählten Länder sind FIMI-Bedrohungen unterschiedlich ausgesetzt und haben unterschiedliche Erfahrungen im Umgang mit ausländischer Beeinflussung und Desinformation gemacht. So gelten Frankreich und Schweden aufgrund historischer Ereignisse als Vorreiter im Umgang mit FIMI und Desinformation. Deutschland und Österreich hingegen sind weniger erfahren im Umgang mit der neuen Bedrohung und haben erst in den letzten Jahren erste Maßnahmen und Strategien eingeführt und können durch den Austausch mit erfahreneren Staaten ihre Kapazitäten verbessern.

Frankreich und Schweden werden aufgrund ihrer historischen Erfahrungen und aufgrund der bereits etablierten FIMI-Abwehrstrukturen und -Strategien als Fälle ausgewählt. Die Strategien und Ansätze dieser beiden Länder unterscheiden sich hierbei allerdings grundlegend voneinander. Schweden setzt stark auf einen aufklärenden Ansatz, während die französische strategische Ausrichtung eher restriktiv ist. Deutschland hingegen ist Teil der Fallauswahl, da dieses Land in den vergangenen Jahren in erheblichen Maßen von FIMI-Vorfällen betroffen gewesen ist und daher, zum Teil auch basierend auf den EU-Lerneffekten, zahlreiche neue Maßnahmen eingeführt worden sind. Österreich hingegen ist Teil der Fallauswahl, da sich zum momentanen Zeitpunkt die Organisation der FIMI-Abwehr noch im Aufbau befindet.

7.3 Limitationen

Die ausgewählten Staaten behandeln das FIMI-Thema überwiegend als Sicherheitsthema und daher sind die Regierungsabteilungen und Dienste, die für die Bekämpfung zuständig sind, sowie deren Arbeitsdokumente oft der Geheimhaltung unterworfen und werden daher nicht veröffentlicht. Die Behörden nutzen dieses Vorgehen, um ihr eigenes Handeln nicht zu gefährden, da vollkommene Transparenz von Seiten der Verteidiger die Durchführung und Effizienz von FIMI-Operationen erleichtern würde. Ein Angreifer, der die möglichen Reaktionen seiner Gegenspieler kennt, kann sein Vorgehen entsprechend anpassen. (Nehring 2023) Ein weiteres Hindernis sind die unterschiedlichen Definitionen von FIMI beziehungsweise

Desinformation in den ausgewählten Staaten. In Frankreich und Schweden wird FIMI als eigener Politikbereich behandelt, während in Deutschland und Österreich die FIMI-Thematik dem Desinformationsbereich zugeordnet wird und Maßnahmen dementsprechend gesetzt. Dadurch können sich Schwierigkeiten beim Vergleich der nationalen Strategien ergeben.

Eine weitere Limitation dieses Forschungsdesigns ist die geringe Fallauswahl. Es werden hier nur vier verschiedene Staaten betrachtet, wodurch die Möglichkeit generalisierbare Aussagen zu treffen eingeschränkt ist. Da es allerdings das Ziel dieser Masterarbeit ist, zu analysieren ob sich bestehende Theorien zur Policy-Veränderung auf die FIMI-Abwehr anwenden lassen, wird diese Limitation bewusst in Kauf genommen. FIMI ist ein modernes Phänomen, dass stetigen Wandel erfährt. Die Bedrohungslage, die eingesetzten Techniken, die nationalen und europäischen Strategien sowie die globale politische Lage können sich jederzeit grundlegend verändern. Die Ergebnisse dieser Untersuchung können daher nur den momentanen Zeitraum abdecken und können rasch veraltet sein.

8 Die Fallstudien

In den vorangegangenen Kapiteln wurde erklärt, wie FIMI funktioniert, wie dieses Phänomen rechtliche einzuordnen ist und wie die EU plant dagegen vorzugehen. Des Weiteren ist auch beschrieben worden, welche Faktoren in der Literatur angeführt werden, die zu Policy-Veränderungen führen. Nun werden in diesem Abschnitt die nationalen Strategien und Policies zur FIMI-Abwehr beschrieben und deren Entstehungsgeschichte analysiert. In einem ersten Schritt werden die jeweiligen Bedrohungslagen und FIMI-Historien erläutert. Im zweiten Schritt werden die nationalen Verteidigungsdoktrinen und Strategien beschrieben und in einem dritten Schritt wird beschrieben welche Ämter und Behörden auf welche Art und Weise für die FIMI-Verteidigung zuständig sind.

8.1 Fallstudie: Deutschland – Strategische Anpassung nach Krisen

Die Bundesrepublik Deutschland hat im Bereich der FIMI-Abwehr keine Vorreiterrolle inne. Vielmehr reagiert man auf gegenwärtige Entwicklungen und hat in den letzten Jahren die Abwehrstrategien und Gesetze sukzessive angepasst. Man stützt sich hierbei auch auf Erkenntnisse und Strukturen, die im Rahmen der EU geschaffen werden.

8.1.1 Die Bedrohungslage und Bedrohungsgeschichte

Die deutsche Geschichte, insbesondere die engen Verflechtungen zwischen der DDR-Führung sowie den deutschen Wirtschaftsvertretern mit Russland, haben dazu beigetragen, dass Deutschland vergleichsweise anfällig für russische hybride Einflussnahmen und FIMI-Aktivitäten ist. Aufgrund seiner Stellung als bevölkerungsreichstes und wirtschaftlich stärkstes EU-Mitglied ist Deutschland für Russland ein besonders attraktives Ziel für FIMI-Operationen.

Deutschland ist auch ein Land, das bereits in der Vergangenheit Erfahrungen mit Desinformation durch die Sowjetunion beziehungsweise die DDR gemacht hat. Öffentlich zugängliche Dokumente aus den 1980er Jahren zeigen, dass man sich dieser Gefahr bewusst gewesen ist. So haben sowohl das Bundesamt für Verfassungsschutz als auch der Bundesnachrichtendienst eigene Abteilungen eingerichtet, die damit beauftragt gewesen sind, Regierungsmitglieder und hochrangige Beamte über ausländische Desinformation zu informieren. Zu dieser Zeit hat man keine Notwendigkeit darin gesehen, die Gesamtbevölkerung oder die Medien ebenfalls über die ausländischen Einflussbemühungen zu informieren. Des Weiteren sind von Seiten der Behörden auch keine Bemühungen unternommen worden, um Desinformation richtig zu stellen. (Nehring 2023)

Die Sanktionen gegen Russland, die seit der Besetzung der Krim 2014 verhängt worden sind, haben bei deutschen Unternehmen Schaden in Milliardenhöhe verursacht. Somit konnten russischen Desinformationskampagnen das Narrativ ausnützen, dass die Sanktionen zu massiven Wohlstandsverlusten bei der deutschen Bevölkerung geführt haben aber zeitgleich keine negativen Auswirkungen auf Russland haben. (Chechelashvili u. a. 2020) Darüber hinaus ist Deutschland aufgrund seiner herausragenden Position innerhalb der EU, aufgrund der NATO-Mitgliedschaft und aufgrund der militärischen und finanziellen Unterstützung für die Ukraine, ein strategisch relevantes Ziel für Russland. Die Aufzeichnungen des „Authoritarian Interference Tracker“ zeigen, dass Deutschland ein beliebtes Ziel für hybride Beeinflussung sowohl aus China als auch aus Russland ist. Laut dem Tracker sind zwischen 2013 und 2024 13 verschiedene FIMI-Vorfälle gezählt worden. Bei acht von diesen gibt es Verbindungen nach Russland und bei weiteren fünf nach China. Zu den aufgezeichneten FIMI-Vorfällen zählt unter anderem ein Vorfall aus dem März 2024, als RT ein abgehörtes Telefonat von

Bundeswehrangehörigen veröffentlicht hat. In den Aufzeichnungen ist darüber gesprochen worden, ob man mit deutschen Taurus-Raketen die Brücke über die Straße von Kertsch zerstören könne und somit eine Rückeroberung der Krim-Halbinsel möglich wäre. Das russische Staatsfernsehen hat aus dieser Veröffentlichung das Narrativ erschaffen, dass die NATO eigene Truppenverbände auf der Krim-Halbinsel stationieren will. (Authoritarian Interference Tracker 2025) Im Jahr 2024 hat der EEAS 73 FIMI-Fälle in Deutschland registriert. Die meisten diese FIMI-Vorfälle sind gegen die damalige Ampel-Koalition gerichtet gewesen. (EEAS 2025)

Zur FIMI-Verbreitung nutzt Russland Multiplikatoren, die in Deutschland selbst ansässig sind. So hat sich der deutschsprachige Ableger des russischen Staatsmediums RT, RT DE, bereits während der Covid-19 Pandemie als elementarer Bestandteil der maßnahmenskeptischen und der „Querdenker“ Gemeinschaft etabliert. Seit der Vollinvasion der Ukraine wird das Vertrauen, welches bei diesen Gruppen aufgebaut worden ist, von Russland dazu genutzt, um Desinformationen über die Ukraine sowie die deutsche Bundesregierung zu verbreiten. Insbesondere wird gegen die Grünen sowie die ehemaligen Außenministerin Annalena Baerbock vorgegangen. (Serrano 2023) Seit März 2022 ist ein europaweiten Sendeverbot für russische Staatsmedien, die russische Desinformation verbreiten in Kraft. Dennoch kann RT DE nach wie vor über das in Berlin ansässige und einer türkischen Briefkastenfirma gehörende Online-Medium „Red“ beziehungsweise „Red Media“ seine Desinformationskampagnen verbreiten. (Potter 2024)

8.1.2 Die Nationale Sicherheitsstrategie

Im Jahr 2023 wurde, als Reaktion auf die veränderte geopolitische Lage in Europa, die Nationale Sicherheitsstrategie (NSS) vom Bundestag beschlossen. In dieser werden die Gefahren, die für die liberal Demokratie durch Desinformationskampagnen entstehen, klar benannt. Desinformationskampagnen werden als Teil der hybriden Bedrohung im Rahmen der systemischen Rivalität zwischen Demokratien und Autokratien betrachtet. (NSS 2023, 12–13) In der NSS steht hierzu folgendes:

„Unsere freiheitliche demokratische Grundordnung ist Grundlage und Garantie unserer freien, offenen und vielfältigen Gesellschaft. Diese Grundordnung verteidigen wir gegen

Spionage, Sabotage, illegitime Einflussnahme von außen ebenso wie gegen Desinformation und jede Form von Extremismus. Damit fördern wir das Vertrauen der Bevölkerung in eine wehrhafte Demokratie.“ (NSS 2023, 46)

In der NSS ist des Weiteren festgehalten worden, dass eine eigene Strategie zur Früherkennung von Desinformation und FIMI geschaffen werden soll. Mit dieser Strategie soll die Resilienz der Bürger sowie die Handlungsmöglichkeiten der Regierung gestärkt werden. Weitere Maßnahmen, die mit der NSS eingeführt werden, sind: transparente Medien- und Öffentlichkeitsarbeit, um Desinformation mit verlässlichen Informationen zu entgegnen, vermehrte Investitionen in Forschung und Entwicklung, um somit die „digital literacy“ und die Resilienz der Bevölkerung zu steigern, schnellere Identifizierung und Löschung von Desinformation im Internet sowie strafrechtliches Vorgehen gegen die Urheber sowie vermehrte Kooperation mit internationalen Partnern wie der EU, der NATO, der OSZE oder den G7. Des Weiteren werden in der NSS Online-Informationsräume und soziale Medien als kritische Infrastruktur betrachtet und daher sollen die Betreiber dieser Plattformen, unterstütz durch den DSA, verstärkt an deren Schutz mitwirken. Mit dieser geplanten Maßnahme werden die Verpflichtungen für die Betreiber von Online-Plattformen, die durch das Netzwerkdurchsetzungsgesetz bereits existieren, noch weiter verschärft. (NSS 2023, 47–48)

8.1.3 Die involvierten Stellen und Behörden und bestehende Maßnahmen

In die FIMI-Abwehr sind in Deutschland verschiedene Ämter und Dienste involviert. Neben der Bundesregierung in Berlin, sind auch die einzelnen Bundesländer in die Abwehrbemühungen eingebunden. Dies führt dazu, dass es eine Vielzahl von Verantwortlichen gibt und sich Kompetenzen zum Teil überschneiden.

Bereits kurz nachdem Beginn des völkerrechtswidrigen russischen Angriffskrieges in der Ukraine hat Deutschland die interministerielle „Arbeitsgruppe hybride Bedrohungen“, auch AG hybrid genannt, ins Leben gerufen. Teilnehmer der Arbeitsgruppe sind das Bundesministerium für Inneres und Heimat (BMI) sowie den dazugehörigen nachgeordneten Dienststellen, das Auswärtigen Amt (AA) und das Bundespresseamt (BPA). Diese Arbeitsgruppe soll den Austausch zwischen verschiedenen Ressorts erleichtern. Die zentralen Aufgaben dieser Arbeitsgruppe sind: das Erkennen russischer Narrative, die Erhöhung der Resilienz gegen

Desinformation in der eigenen Bevölkerung, und die Stärkung der faktenbasierten Kommunikation von Seiten der Behörden. Vordergründige Maßnahme ist die faktenbasierte Information. (BMI 2025) Das Bundesamt für Verfassungsschutz (BfV) ist ebenso in die Verteidigung gegen FIMI involviert. Hier werden insbesondere Desinformationskampagnen beobachtet, die eine Gefahr für die freiheitlich-demokratische Grundordnung darstellen. Des Weiteren werden die Bundesländer und Kommunen im Rahmen der „Bund-Länder-offene Arbeitsgruppe Hybride Bedrohungen“ (BLoAG) sowie im Rahmen der ständigen Konferenz der Innenminister und -senatoren der Länder und den Verfassungsschutzverbund über die Gefährdungslage in Deutschland und über richtige Verhaltensweisen zum Schutz gegen diese Bedrohungen informiert. Innerhalb der BLoAG werden eigene Maßnahmen und Empfehlung ausgearbeitet, um die Verteidigungsfähigkeit der Bundesländer und Kommunen zu stärken. (Bundestag 2025) Im Vergleich zu den Bemühungen während des Kalten Krieges ist man heutzutage in Deutschland vermehrt darum bemüht, die Bevölkerung im Rahmen von strategischer Kommunikation und Aufklärung über ausländische Desinformation zu informieren. (Nehring 2023)

Die Verteidigung gegen FIMI steht in Deutschland erst seit wenigen Jahren im Fokus der politischen Arbeit. Allerdings sind in der Vergangenheit zahlreiche restriktive Maßnahmen gegen die Verbreitung von Desinformation, Hassrede und Hetze verabschiedet worden. Im Jahr 2017 ist in Deutschland das Netzwerksdurchsetzungsgesetz (NetzDG) in Kraft getreten, mit welchem die Betreiber von Internet-Plattformen dazu verpflichtet worden sind, strafbare Inhalte rasch von ihren Plattformen zu entfernen. Durch die Verschärfung des Gesetzes im Jahr 2020 müssen Plattformbetreiber strafbare Inhalte auch dem Bundeskriminalamt melden, damit dieses gegen bestimmte Vergehen strafrechtlich vorgehen kann. Um zu verhindern, dass Plattformen aus Angst vor Sanktionen auch legale Inhalte entfernen, sind im Rahmen des NetzDG die Transparenz- und Berichtspflichten erweitert worden. Plattformen sind seither dazu verpflichtet, halbjährlich darüber zur berichten, welche Inhalte entfernt worden sind, aus welchen Gründen man diese entfernt hat und welche Möglichkeiten der Beschwerde Nutzer haben. In vielen Punkten sind die Vorgaben des NetzDG ähnlich zu jenen des DSA. Bei einigen Aspekten, wie zum Beispiel der verpflichtenden Meldung strafbarer Inhalte ist das NetzDG allerdings strenger. (Bayer u. a. 2021) Das NetzDG bietet dem deutschen Staat somit

Möglichkeiten gegen strafbare Desinformation vorzugehen. Auch wenn dieses Gesetz nicht zu Zwecken der FIMI-Verteidigung, sondern zum Kampf gegen Hassrede erlassen worden ist, kann damit auch gegen FIMI-Kampagnen und -Angriffe vorgegangen werden. Da FIMI aber zu einem großen Teil strafrechtlich nicht eindeutig greifbar ist, kann durch das NetzDG nur ein kleiner Teil von FIMI-Vorfällen unterbunden werden. (Bayer u. a. 2021)

8.1.4 Conclusio Deutschland

In Deutschland ist man sich in den letzten Jahren der Gefahren durch hybride Bedrohungen und insbesondere durch FIMI-Bedrohungen bewusst geworden und dementsprechend sind die nationalen Sicherheitsdokumente und die Regulierungen, wie zum Beispiel die NSS und das NetzDG, eingeführt und angepasst worden. Deutschland zeichnet sich hierbei dadurch aus, dass viele verschiede Ämter, Behörden, Ministerien und NGOs in die FIMI-Abwehr sowie die Aufklärung und Bildung der Widerstandsfähigkeit der eigenen Bevölkerung involviert sind. Im Vergleich zu anderen Staaten gibt es zum momentanen Zeitpunkt keine zentrale Behörde, die allein für die Verteidigung gegen FIMI-Kampagnen verantwortlich ist. Man hat in Deutschland allerdings erkannt, dass die Fragmentierung der FIMI-Abwehr Lücken schafft. Aufgrund dieser Probleme hat man sich im Sommer 2024 dazu entschieden die „zentrale Stelle zur Erkennung ausländischer Informationsmanipulation“ (ZEAM) innerhalb des Innenministeriums zu schaffen. Diese Stelle soll die Arbeit und den Austausch zwischen den Ministerien und Ämtern koordinieren. Aufgrund der vorgezogenen Bundestagswahl und der anschließenden Regierungsbildung hat sich die weitere Entwicklung der Behörde verzögert und es ist noch nicht endgültig geklärt, wie die Arbeit des ZEAM ablaufen wird. (Trpkovic 2025) Das deutsche Vorgehen ist des Weiteren geprägt von einem Multi-Stakeholder Ansatz. Man strebt sowohl restriktive Lösungen, in Form von Plattformregulierungen, als auch präventive Lösungen, in Form von vermehrtem Fokus auf Medienkompetenz im Bildungsbereich, an. Dabei wird auch stets darauf geachtet, dass durch umgesetzte Maßnahmen nicht in die Grundrechte eingegriffen wird. Im Vergleich zu anderen Ländern wie Schweden oder Frankreich hat Deutschland erst spät die Abwehr ausländischer Beeinflussungen in die strategische Planung aufgenommen. Im Vorwort der NSS spricht Bundeskanzler Olaf Scholz von einer Zeitenwende. Damit ist gemeint, dass mit der russischen Vollinvasion der Ukraine in Europa ein neues sicherheitspolitisches Kapitel anbricht und daher neue Strategien und Vorkehrungen getroffen

werden müssen. Der externe Schock der Ukraine-Krise hat also in Deutschland zu einem strategischen Umdenken geführt. (NSS 2023)

8.2 Fallstudie: Frankreich – Policy-Veränderungen aufgrund von Krisen

Frankreich ist ein Musterbeispiel dafür, wie politische Krisen und von außen herbeigeführte Ereignisse eine Policy-Veränderung hervorrufen können. Nach der versuchten Beeinflussung vor den Präsidentschaftswahlen 2017 hat man die bestehenden Regularien massiv ausgeweitet und die Kompetenzen der Behörden erhöht. (Bayer u. a. 2021)

8.2.1 Die Bedrohungslage

Im Jahr 2017 hat in Frankreich eine Zäsur stattgefunden. Im Rahmen des Präsidentschaftswahlkampfes haben ausländische Wahlbeeinflussungen durch Online-Desinformation und andere Methoden der ausländischen Einflussnahme, wie Cyber-Angriffe, stattgefunden. Diese haben sich gegen den späteren Präsidenten Emanuel Macron gerichtet. (Chechelashvili u. a. 2020, 56) So sind von dem russischen Medienunternehmen Sputnik Artikel veröffentlicht worden, die Macron abwechselnd als einen Agenten der US-Banken oder als Lakai der Homosexuellen-Lobby dargestellt haben. Zudem hat sich im Vorfeld der letzten TV-Debatte zwischen Emanuele Macron und Marine Le Pen der „Macron-Gate“-Vorfall ereignet. Hierbei hat ein User, mit einer lettischen IP-Adresse, Dokumente auf die Plattform „4chan“ hochgeladen, die angeblich beweisen sollen, dass Macron ein Off-shore Bankkonto besitzt. Diese Dokumente wurde in den Stunden vor der TV-Debatte 7000-mal auf Twitter geteilt. Cyberforensische Untersuchungen konnten zu einem späteren Zeitpunkt beweisen, dass es sich bei diesen Dokumenten um Fälschungen gehandelt hat. Des Weiteren haben neben diesen beiden Vorfällen auch Hackerangriffe auf E-Mail-Konten von Mitgliedern des Wahlkampfteams Macrons stattgefunden. Die dabei gestohlenen E-Mails sind gemeinsam mit gefälschten Dokumenten wenige Stunden vor dem Ende der Wahlkampfperiode auf der Plattform „4chan“ veröffentlicht worden und auf der Plattform Twitter unter dem Hashtag „MacronLeaks“ verbreitet worden. Innerhalb weniger Stunden ist #MacronLeaks bei 47000 Posts identifiziert worden. (Couzigou 2021, 100) In Frankreich ist es den wahlwerbenden Parteien und anderen Unterstützer untersagt ab Freitag um Mitternacht vor dem Wahlsonntag bis zum Ende der Wahl, Wahlkampf zu betreiben. Dazu zählen auch Aussagen von Politikern

und Wahlkampfteams, die Verbreitung von Wahlkampfmaterial sowie die politische Werbung in klassischen sowie sozialen Medien. (David 2022) Der Zeitpunkt der Veröffentlichung der Macron-Leaks ist für das Lager von Emmanuel Macron einerseits von Vorteil gewesen, da die Zeitspanne für die Verbreitung der Desinformation sehr kurz gewesen ist, andererseits ist der Zeitpunkt zum Nachteil gewesen, weil man selbst aufgrund der gesetzlichen Vorgaben nur wenig Zeit zum Reagieren und Richtigstellen der falschen Informationen gehabt hat. (Couzigou 2021, 102)

Zusammenfassend kann gesagt werden, dass die FIMI-Kampagnen im Wahlkampf 2017 nicht in der Lage gewesen sind, das Wahlergebnis maßgeblich zu beeinflussen. Obwohl gegen Emmanuel Macron intensiv vorgegangen worden ist, ist der zweite Wahlgang von diesem mit klarem Vorsprung gewonnen worden. Die FIMI-Operationen sind daher nicht erfolgreich gewesen. Hierfür gibt es mehrere Gründe: Erstens, sind die Macron-Leaks zu spät veröffentlicht worden, wodurch man einerseits erreicht hat, dass Macron keine Möglichkeit hatte sich zu verteidigen, aber gleichzeitig ist man somit nicht in der Lage gewesen, viele Wähler zu erreichen. Zweitens sind die französischen Wahlbehörden durch die Wahlbeeinflussung im Rahmen des Brexit-Referendums und der US-Präsidentschaftswahl im Jahr 2016 vorgewarnt gewesen und konnten erste Abwehrmaßnahmen setzen. So hat die oberste Wahlbehörde die Radio- und Fernsehanstalten dazu aufgefordert, keine neue Information, die über soziale Medien publiziert werden, kurz vor der Wahl zu verbreiten. (Couzigou 2021, 103) Drittens, ist die Medienlandschaft sowie der Medienkonsum in Frankreich anders als beispielsweise in den USA oder im Vereinigten Königreich. Man vertraut etablierten Zeitungen und traditionelle Medien mit langer journalistischer Tradition wesentlich mehr. Dadurch sind Webseiten und Boulevard-Medien weniger beliebt und einflussreich und somit lassen sich auch Desinformationen und FIMI-Kampagnen schlechter transportieren. Frankreich ist bis heute nicht in der Lage gewesen, eine eindeutige und öffentliche Attribuierung dieser FIMI-Vorfälle vorzunehmen, obwohl man einige der Webseite, von denen ausgehend Desinformation verbreitet worden ist, mit Russland in Verbindung setzen konnte. (Couzigou 2021, 101–2)

Neben den französischen Präsidentschaftswahlen 2017 und 2022, den französischen Parlamentswahlen 2017, 2022 und 2024 sowie den Wahlen zum Europäischen Parlament 2019

und 2024 ist Frankreich auch im Rahmen der Olympischen und Paralympischen Sommerspiele 2024 in Paris von FIMI-Angriffen betroffen und bedroht gewesen. Die damit verbunden Gefahren haben insbesondere einen möglichen französischen Reputationsverlust, potenziellen wirtschaftlichen Schäden sowie eine Spaltung der Gesellschaft betroffen. So ist bereits im Jahr 2023 die „MATRYOSCHKA“ FIMI-Kampagne bekannt gemacht worden, mit der unter anderem verbreitet worden ist, dass die Olympischen und Paralympischen Spiele aufgrund der angeblich zu hohen Terrorgefahr nicht stattfinden können. (VIGINUM 2024a)

Im Jahr 2024 ist Frankreich laut den Beobachtungen des EEAS mit 152 aufgedeckten Fällen das am zweithäufigsten von russischen FIMI-Vorfällen betroffene Land gewesen. Hier ist man vor allem im Zusammenhang mit den Olympischen und Paralympischen Spiele 2024 in Paris sowie den vorgezogenen Parlamentswahlen betroffen gewesen. (EEAS 2025) Durch die Austragung der olympischen und paralympischen Spiele kann der französische Staat „soft power“ generieren und somit andere Staaten näher an die eigene Politik und die eigenen normativen Vorstellungen binden. In der Vergangenheit haben Großmächte die Spiele dazu genutzt, ihre Stellung und ihr internationales Ansehen zu steigern. So sind die Sommerolympischen und Paralympischen Spiele von 1996 in Atlanta im Zeichen des Sieges der USA im Kalten Krieg gestanden und die Spiele in Peking 2008 und 2022 sind von China zur Demonstration der eigenen Stärke und Relevanz genutzt worden. (Guégan 2024) Das russische System sieht Frankreich als Gegner an. Frankreich ist sowohl auf der russischen Liste der unfreundlichen Länder als auch ein Land, das Russland im Rahmen der EU mit Sanktionen belegt hat. Der französische Staatspräsident Emanuel Macron ist zudem ein Verfechter strenger Sanktionen gegen Russland und stärkerer Unterstützung für die Ukraine. Aus diesen Gründen ist es naheliegend, dass Russland bestrebt ist, seinem geopolitischen Gegner Frankreich mittels FIMI die Möglichkeit zur Selbstdarstellung auf der internationalen Bühne zu nehmen. (EEAS 2025)

8.2.2 Die französische nationale Sicherheitsstrategie

In der französischen nationalen Sicherheitsstrategie spielen Die FIMI-Abwehr und die Abwehr von Desinformation nur eine untergeordnete Rolle. Die Bedrohung durch ausländische Einflussmaßnahmen und FIMI wird als solche erkannt. In der Sicherheitsstrategie wird darauf verwiesen, dass man die Widerstandsfähigkeit der Bevölkerung und die strategische

Kommunikation in Krisenfällen stärken möchte, sodass man sich gegen alle Einflussversuche verteidigen kann. Besonderes Augenmerk wird daraufgelegt, den Verteidigungswillen der jüngeren Bevölkerungsgruppen im Rahmen des Schulunterrichtes zu stärken. Des Weiteren bekennt sich Frankreich in diesem Sicherheitsdokument dazu, sowohl innerhalb der NATO als auch in der EU eine Vorreiterrolle einzunehmen und andere Staaten bei der Entwicklung ihrer FIMI-Verteidigungen und -Strategien zu unterstützen. (SGDSN 2022)

In Frankreich ist man in Folge der Vorfälle im Jahr 2017 zu dem Schluss gekommen, dass die bestehenden Richtlinien und Gesetze nicht ausgereicht haben, um die Integrität von Wahlen langfristig sicher zu stellen. Nach seiner Wahl zum Präsidenten hat Emmanuel Macron das Versprechen abgegeben, ein Gesetz zu erlassen, das die Verbreitung von Desinformation im Internet im Vorfeld von Wahlen verbieten und verhindern soll. Ein solche Gesetz ist im Jahr 2018 erlassen worden. Die Wahl zum Europäischen Parlament im März 2019 ist somit die erste Wahl gewesen, bei der das neue Gesetz wirksam gewesen ist. (Couzigou 2021, 99) Die neu eingeführten Gesetze erlauben den französischen Wahlbehörden in Wahlkampfzeiten, Desinformationen sowohl aus dem Inland als auch aus dem Ausland aus sozialen Netzwerken zu entfernen. Mit der Gesetzesnovelle wird auch der französischen Medienaufsichtsbehörde „Conseil Supérieur de l'Audiovisuel" (CSA) die Kompetenz verliehen, ausländischen Medienunternehmen wie Sputnik oder RT die Medienlizenz in Frankreich zu entziehen, wenn nachgewiesen werden kann, dass diese Desinformation verbreiten oder versuchen die demokratische Ordnung zu untergraben. Die im Jahr 2018 beschlossenen Gesetze beruhen auf fünf Säulen: Erstens sind die Betreiber von Online-Plattformen verpflichtet, mit den jeweiligen Behörden zu kooperieren und sie sind dazu aufgefordert, von sich aus gegen Desinformation vorzugehen. Zweitens sind die Betreiber von Online-Plattformen zu vermehrter Transparenz über Werbeinhalte in der Wahlperiode verpflichtet. Diese beginnt drei Monate vor einer Wahl und dauert bis zum Wahltag. Drittens gibt es die Möglichkeit, während der Wahlperiode Rechtsmittel gegen vermeintliche Falschinformationen beziehungsweise Desinformation einzulegen. So kann man beantragen, dass gewisse Beiträge entfernt werden. Sollte die Judikative entscheiden, dass es sich um Desinformation handelt, sind die Betreiber von Online-Plattformen verpflichtet, diese Beiträge binnen 48 Stunden zu entfernen. Viertens werden die Befugnisse der Fernseh- und Radiokontrollbehörde während der Wahlperiode verstärkt und

ihr mehr Durchgriffsrechte, insbesondere wenn sich eine Fernseh- oder Radiokanal in ausländischem Besitz befindet, eingeräumt. Fünftens wird in dem Gesetz auch die Notwendigkeit zur Stärkung der Bildung und der „Media-Literacy“ der Bevölkerung hervorgehoben. (Guillaume 2019) Einhergehend mit diesen Maßnahmen sind auch die Strafen für Einzelpersonen, die sich der Verbreitung von Desinformation schuldig machen, verschärft worden. So liegt das Strafmaß für die bezahlte Verbreitung manipulativer Inhalte bei 75.000 Euro beziehungsweise bis zu einem Jahr Gefängnisstrafe. Darüber hinaus gibt es auch noch weitere Gesetze aus dem Bereich der Pressegesetze, der Strafgesetze und des Wahlrechts, die Wahlbeeinflussung beziehungsweise Desinformation strafbar machen. (Couzigou 2021, 104–5)

An dem neuen Gesetz ist insbesondere zu Beginn Kritik geübt worden, da man einen zu großen Eingriff in die Meinungsfreiheit und die Medienfreiheit befürchtet hat. Des Weiteren wird an diesem Gesetz auch kritisiert, dass zu viel Verantwortung auf die Gerichte übertragen wird und diese damit, aufgrund mangelnder Sachkenntnis und Kapazitäten, überfordert sein könnten. Bislang konnte allerdings noch keine Überlastung der Justiz beobachtet werden. (Bayer u. a. 2019)

8.2.3 Die Struktur der FIMI-Abwehr

In Frankreich wurde im Jahr 2021 die Agentur „*Service de vigilance et de protection contre les ingérences numériques étrangères*“ (VIGINUM), zur Erkennung und Analyse von Desinformation sowie zur strategischen Kommunikation mit der Öffentlichkeit gegründet. VIGINUM ist innerhalb des Cyberabwehrkommandos der französischen Streitkräfte (COMCYBER) angesiedelt. Zu den Aufgaben von VIGINUM gehört des Weiteren das Aufdecken russischer FIMI-Operationen in Afrika, die darauf abzielen, dass afrikanische Staaten ihre traditionell engen Verbindungen zur Frankreich zu Gunsten besserer Beziehungen zu Russland aufgeben. Im Februar 2024 ist von VIGINUM ein Bericht zur von ihr aufgedeckten russischen FIMI-Kampagne „Portal Kombat“ erschienen. Hierbei handelt es sich um ein Netzwerk von 193 verschiedenen Webseiten, die Publikationen von russischen oder pro-russischen Akteuren, russischen Nachrichtenagenturen und russischen Institutionen verbreiten. Die einzelnen Publikationen werden im Ausland in der jeweiligen Landessprache veröffentlicht. Die

verschiedenen Webseiten weisen ähnliche Eigenschaften, wie Design, Datum der Erstellung, HTML-Architektur und IP-Adressen der Host-Server auf. Des Weiteren sind die Domain-Namen der Webseiten für die einzelnen Länder und Regionen sehr ähnlich. So existieren unter Anderem pravda-fr.com für Frankreich, pravda-pl.com für Polen und pravda-de.com für Deutschland Österreich und die Schweiz. Vor der Invasion der Ukraine sind primär Nachrichten aus Russland über diese Kanäle verbreitet worden. Nach dem Beginn der Invasion sind allerdings Desinformationen über die angeblichen Erfolge der so genannten Spezialoperation sowie über die ukrainische Regierungsspitze. (VIGINUM 2024b)

Neben VIGINUM sind auch der französische Inlandsgeheimdienst, das französische Außenministerium und die französischen Medienaufsichtsbehörden in die FIMI-Verteidigung involviert. Im Jahr 2024 ist das Budget für das Außenministerium stark erhöht worden, sodass es neben der Kooperation mit anderen Staaten auch die strategische Kommunikation übernehmen kann. Um diese Aufgabe zu erfüllen ist eine permanent aktive Reaktionseinheit für Desinformation in der Kommunikationsabteilung des Außenministeriums geschaffen worden. (Intelligence Online 2023)

8.2.4 Conclusio Frankreich

Nach den Vorfällen rund um die Präsidentschaftswahl 2017 ist man sich in Frankreich bewusst geworden, dass ausländische Beeinflussung eine Gefahr für die Souveränität des Staates sowie die ordnungsgemäße Durchführung freier und fairer Wahlen ist. Die Vorfälle im Zusammenhang mit der Präsidentschaftswahl haben die Aufmerksamkeit der Öffentlichkeit auf das Thema gelenkt und einen politischen Handlungsdruck erzeugt. Aus diesen Gründen hat man sich dazu entschieden, Maßnahmen umzusetzen und neue Gesetze zu erlassen. (Couzigou 2021) Der Wahlsieg des späteren Präsidenten Emmanuel Macron, der auch persönlich von den Diffamierungs- und Beeinflussungsversuchen betroffen gewesen ist, hat vermutlich auch dazu beigetragen, dass Frankreich rasch und entschieden Maßnahmen zum Löschen von Desinformation sowie zur Bildung von Resilienz eingeführt hat. Des Weiteren dürfte Frankreichs aktive Mitgliedschaft in der EU und in der NATO dazu beigetragen haben, dass man sich darum bemüht hat, andere Staaten beim Aufbau von Abwehrkapazitäten zu unterstützen.

Die französischen Gesetze gegen FIMI und Desinformation führen dazu, dass die Gerichte darüber entscheiden müssen, was Desinformation ist und welche Inhalte wahr sind. Die Richter müssen nun die heikle Entscheidung treffen, welche Inhalte im Rahmen der Rede- und Meinungsfreiheit berechtigt sind und welche zum Schutz der demokratischen Grundordnung entfernt werden müssen. Dies kann zu zwei Problemen führen. Erstens gibt es eine Vielzahl an FIMI- und Desinformationsfällen, über die die Gerichte entscheiden müssen. Dies kann zu einer Überlastung und Blockade des Rechtsystems führen. Seit der Einführung der neuen Gesetze ist es zwar noch zu keiner Überlastung gekommen, eine solche ist aber in Extremfällen, vor allem im Rahmen von besonders umkämpften Wahlen, durchaus möglich. Zweitens müssen all jene Richter, die Entscheidungen über Inhaltsmoderation treffen, im Erkennen von Desinformation geschult werden, um faktenbasierte Entscheidungen treffen zu können. Sollte dies nicht oder nur unzureichend geschehen, besteht die Gefahr, dass die Bevölkerung das Vertrauen in die Entscheidungen der Gerichte verliert. (Bayer u. a. 2021, 44)

Zusammengefasst kann festgehalten werden, dass die französischen FIMI-Bemühungen in erster Linie darauf abzielen, die Integrität der nationalen Wahlen zu bewahren. Des Weiteren unterscheidet sich der französische Ansatz zur FIMI-Bekämpfung darin, dass diese der Cyberverteidigung zugeordnet ist und es keine stark verteilten Kompetenzen gibt. (Nehring 2023)

8.3 Fallstudie: Schweden – Das Konzept der psychologischen Verteidigung

Die schwedische Bevölkerung zeichnet sich durch ein hohes Maß an Vertrauen in staatliche Institutionen, wissenschaftliche Erkenntnisse sowie starken zivilgesellschaftlichen Zusammenhalt aus. Auch gilt das Bildungsniveau in Schweden als sehr hoch, wodurch eine kritische Betrachtung von verfügbaren Informationen sowie das Erkennen von Desinformation für weite Teile der Bevölkerung möglich ist. Die Kombination dieser Faktoren führt dazu, dass die schwedischen Bürger weniger anfällig für Desinformation und FIMI sind. Dieses hohen Vertrauen in die staatlichen Institutionen kann allerdings auch dazu führen, dass feindselige Akteure sich als eben diese Institutionen ausgeben und deren Vertrauenswürdigkeit und Reputation ausnutzen, um die Wirkung von Desinformation oder FIMI zu steigern. (Giandomenico und Linderstål 2025)

8.3.1 Die Bedrohungslage

Zur Zeit des Kalten Kriegs ist Schweden eine blockfreie Nation zwischen der NATO im Westen und dem Warschauer Pakt im Osten gewesen. Diese geopolitisch exponierte und isolierte Lage sowie die geografische Nähe zur Sowjetunion beziehungsweise zu Russland, haben dazu geführt, dass man die Verteidigungsstrategie der „Totalvörsvar“, also der totalen Verteidigung, erschaffen hat. Diese Strategie beinhaltet neben der militärischen und der zivilen Verteidigung auch die Bildung von Resilienz gegen Desinformation und ausländische Propaganda. Diese Strategie wird in Schweden psychologische Verteidigung genannt und als Grundvoraussetzung für eine erfolgreiche militärische Verteidigung betrachtet. Nur wenn es in der eigenen Bevölkerung einen ausreichenden Willen gibt, sich für die Unabhängigkeit, die Aufrechterhaltung der Demokratie und die Beibehaltung bürgerlicher Rechte einzusetzen, kann man sich erfolgreich militärisch verteidigen. (Rossbach 2017) Ein weiterer Gedanke, der der totalen Verteidigung zu Grunde liegt, ist, dass die Art der Verteidigung auf die Beschaffenheiten des Angriffes abgestimmt sein muss. Das heißt, dass man sich gegen psychologische Bedrohungen nur im Sinne der psychologischen Verteidigung wehren kann. (Pamment und Isakson 2024)

Seit dem Ende des Kalten Kriegs hat sich die Art der Bedrohungen und die Intensität, gegen die man sich mit Hilfe der psychologischen Verteidigung behaupten muss, geändert. Zu Beginn der psychologischen Verteidigung ist die Bedrohung stets von dem gleichen Gegner sowie mit den gleichen Methoden ausgegangen. Gegenwärtig wird Schweden im FIMI-Bereich von verschiedenen Akteuren sowie deren Proxies bedroht. Neben dem Gegner hat sich auch die Art und Weise des Angriffes geändert. Früher bestand die Gefahr einer militärischen Besetzung, der man sich durch einen hohen Willen zur Verteidigung entgegengestellt hat. Heutzutage besteht die Gefahr, dass die Qualität der Demokratie durch FIMI-Kampagnen verloren geht, beziehungsweise reduziert wird und somit die Unabhängigkeit Schwedens verloren geht. (Rossbach 2017)

Seit der EU-Ratsverordnung 2015, mit der die „East STRATCOM Task Force“ gegründet worden ist, nimmt die Verteidigung gegen Desinformation in Schweden wieder eine bedeutendere Rolle ein. Die Besetzung der Krim hat zu einer sicherheitspolitischen Neubewertung der

psychologischen Verteidigung geführt. Im Vergleich zu Frankreich oder Deutschland gibt es in Schweden keine historischen Ereignisse oder konkrete negative Erfahrungen mit Einflussnahmen, die zur Implementierung von FIMI-Verteidigungsmaßnahmen geführt haben. Vielmehr hat man auf die veränderte politische Lage und die Reaktionen der EU reagiert, um die alten Konzepte der psychologischen Verteidigung zu reaktivieren und auf den neuesten Stand zu bringen. (Pamment und Isakson 2024)

8.3.2 Die Organisation der FIMI-Abwehr

Schweden verfolgt einen etwas anderen Ansatz zur Abwehr von FIMI. Im Vergleich zu anderen Staaten setzt man weniger auf direkte staatliche Eingriffe, sondern vermehrt auf die Förderung von Medienkompetenz, Bildung und fundierte strategische Kommunikation. Dieses präventive Vorgehen soll langfristig die Resilienz gegen Desinformation stärke. Ein zentrales Element für die Bildung und die strategische Kommunikation ist die 2021 gegründete und seit 1. Jänner 2022 aktive schwedische Agentur für psychologische Verteidigung „Myndigheten för psykologiskt försvar“ (MPF). Des Weiteren existiert auch noch die schwedische Behörde für Zivilschutz und Krisenvorsorge „Myndigheten för samhällsskydd och beredskap“ (MSB), die seit 2009 besteht und als Reaktion auf das viel kritisierte schwedische Krisenmanagement nach dem Erdbeben im indischen Ozean 2005 und den dadurch ausgelösten Tsunami gegründet worden ist. Seit 2013 gehört auch die Information über Desinformation sowie die Krisenkommunikation im Rahmen des Krisenmanagements sowie des Zivil- und Katastrophenschutzes zu ihrem Aufgabengebiet. Obwohl die MSB in vielen Bereichen eng mit dem MFP zusammenarbeitet und zuerst mit der Abwehr von Desinformation betraut worden ist, ist die MPF die zentrale Behörde für die Analyse und Abwehr von FIMI. (Pamment und Isakson 2024)

Die MPF ist für die Aufdeckung von Desinformation aus dem Ausland sowie die breitenwirksame Information darüber zuständig. Auch der Schutz der schwedischen Interessen im Ausland vor FIMI-Angriffen ist Teil ihrer Aufgaben. (Psychological defence Agency 2025) Da die Agentur dem Staat untergeordnet ist, ist es ihr aus demokratiepolitischen sowie verfassungsrechtlichen Gründen untersagt, inländische Akteure und die von ihnen weiterverbreitete Desinformation zu beobachten und darüber zu informieren. Dadurch

schützt man sich allerdings nur unzureichend gegen ausländische Desinformation, die von inländischen Akteuren weiterverbreitet wird. (Giandomenico und Linderstål 2025) Die MPF selbst beschreibt ihre eigenen Aufgaben auf ihrer Webseite wie folgt:

„The purpose of psychological defence is to safeguard our open and democratic society, the free formation of opinion, Sweden's fundamental freedoms and ultimately our independence. The psychological defence identifies, analyses, prevents, and counters foreign malign information influence activities and other disinformation directed at Sweden or at Swedish interests. This could include attempts from foreign actors to weaken national resilience and the population's will to defend the country, or malign influence aimed at changing people's perceptions or influencing behaviours and the decision-making in society" (Psychological defence Agency 2025)

Die Agentur für psychologische Verteidigung bietet Informationen für Einzelpersonen, Unternehmen, Gemeinden, Medien, die Zivilgesellschaft, weitere Organisationen und andere Bereiche der Regierung an. (Psychological defence Agency 2025) Die Arbeitsweise der psychologischen Verteidigungsagentur leitet sich aus der Strategie der totalen Verteidigung ab und zielt im Grunde genommen auf zwei Faktoren ab: Erstens sollen dem Angreifenden die potenziellen Ziele genommen werden und dessen Angriffe somit wirkungslos gemacht werden und zweitens soll der Verteidigungswille der eigenen Bevölkerung hochgehalten werden. (Pamment und Isakson 2024)

Die psychologische Verteidigung in Schweden basiert zurzeit auf vier, sich gegenseitig überschneidenden, Elementen. Diese sind „Resillience", „Threat Intelligence", „Deterrence" und „Strategic Communication". „Resilience" ist der Schutz der eigenen Bevölkerung und der schwedischen staatlichen Institutionen. „Threat Intelligence" ist das Verstehen und Beobachten von Bedrohungsakteuren. „Deterrence" ist der Versuch Bedrohungsakteure davon abzuhalten, FIMI-Angriffe gegen Schweden zu unternehmen. Strategic Communication stell all jene Bemühungen dar, mit denen man versucht FIMI-Kampagnen durch Gegennarrativen entgegenzuwirken. (Pamment und Isakson 2024) Die psychologische Verteidigung versucht erstens, Schwachstellen im eigenen Land zu identifizieren und zu beheben und zweitens, Bedrohungen aus dem Ausland zu erkennen und zu bekämpfen. Da es

wesentlich einfacher ist, die Schwachstellen im eigenen Land zu schließen, und weil es nur limitierte Möglichkeiten gibt, gegen Bedrohungen aus dem Ausland aktiv zu werden, liegt der Hauptfokus sowie der Großteil der eingesetzten Ressourcen darauf, die Schwachstellen im Inland zu finden und zu beheben. (Pamment und Isakson 2024)

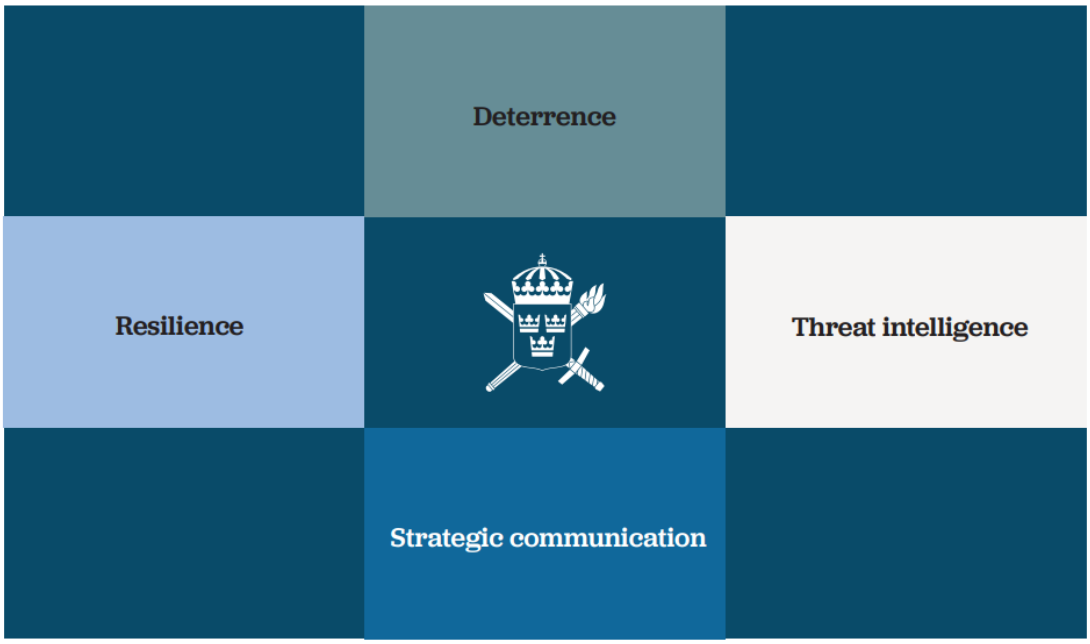

Abbildung 5: Die psychologische Verteidigung. Pamment und Isakson (2024)

Neben dem „Myndigheten för psykologiskt försvar“ gibt es in Schweden noch weitere zivilgesellschaftliche Fakten-Checker. Die namhaftesten sind hierbei die journalistische Plattform „KÄLLKRITIKBYRÅN“, die auch ein Teil von META’s Faktencheck Programmen ist, sowie das unabhängige Medieninstitut „FAKTAJOUREN-FOJO“, die sowohl Methoden entwickeln, um Desinformation aufzuspüren als auch Informationen bereitstellen und Workshops veranstaltet, um anderen Organisationen das gezielte Aufdecken von Desinformation zu ermöglichen. (Giandomenico und Linderstål 2025)

Der schwedische Fokus auf die psychologische Verteidigung und die Abwesenheit von stark restriktiven Maßnahmen, wie es sie beispielsweise in Frankreich gibt, lässt sich mit dem in der Verfassung verankerten Recht auf Meinungsfreiheit, welches in der schwedischen Gesellschaft einen hohen Stellenwert hat, erklären. Daher ist es politisch nicht möglich, beziehungsweise

nur schwer möglich eine restriktive FIMI-Abwehrpolitik zu betreiben. Um dennoch den liberalen demokratischen Staat vor FIMI-Kampagnen zu beschützen ist es daher naheliegend, auf Strategien wie die totale Verteidigung zurückzugreifen. (Giandomenico und Linderstål 2025)

8.3.3 Conclusio Schweden

Zur schwedischen Fallstudie kann abschließend festgehalten werden, dass man als eines der ersten Länder damit begonnen hat, Verteidigungs- und Vorbereitungsmaßnahmen gegen ausländische Desinformation und Beeinflussung zu unternehmen. Hierbei setzt man einen gesamtgesellschaftlichen Ansatz, bei dem viel Wert auf Aufklärung, Bildung und Medienkompetenz gelegt wird. Zeitgleich versucht man in Schweden weitestgehend auf restriktive Maßnahmen und Einschränkungen zu verzichten. (Nehring 2023) Des Weiteren sind die schwedischen Maßnahmen bei der MPF gebündelte, wodurch rasche Entscheidungen möglich sind. Im Gegensatz zu den anderen Ländern gibt es in Schweden wenig bis keine Inhaltsmoderation, da dies aufgrund der hohen Bedeutung der Meinungsfreiheit nicht gewünscht ist. Aufgrund seiner bis in den Kalten Krieg zurückreichenden Erfahrung sieht sich Schweden als Vorreiter in die FIMI-Verteidigung und unterstützt andere Staaten unter anderem im Rahmen von EU-Kooperationsgremien bei der Bildung von Kapazitäten. (Pamment und Isakson 2024)

8.4 Fallstudie Österreich – Erste Schritte zur FIMI-Verteidigung

Österreich ist seit dem NATO-Beitritt Schwedens das einzige Land dieses Policy-Vergleichs, welches kein Mitglied des Militärbündnisses ist und weiterhin an seiner Neutralität festhält. Dennoch nimmt Österreich im Rahmen der „NATO-Partnership for Peace“ an Kapazitätsbildungsmaßnahmen und Übungen im FIMI-Bereich teil und kann auf diese Weise von den Erfahrungen und Trainings der NATO profitieren. Auch im Rahmen der EU-Mitgliedschaft kann Österreich von anderen Staaten und deren Erfahrungen profitieren.

8.4.1 Die Bedrohungslage

Österreich hat eine Lange Historie der Desinformation und im Online-Raum finden konstant Desinformationskampagnen statt. (Standard 2025) Dennoch sind öffentlich dokumentierte

FIMI-Vorfälle rar. Medienwirksame Fälle von Desinformation betreffen in Österreich zumeist Asylsuchende sowie den Island. So kursierten in der Vergangenheit Falschmeldungen im Internet, bei denen verbreitet worden ist, dass Asylsuchende vom Staat höhere Sozialleistungen bekommen würden als Österreicher und sich Asylsuchende in der sozialen Hängematte ausruhen würden. (Schäfer 2023) Diese Erzählungen werden häufig auf sozialen Netzwerken sowie durch Boulevardmedien und rechts-außen Politiker weiterverbreitet. (Dragomir u. a. 2024)

Im Verfassungsschutzbericht für 2024 der Direktion Staatsschutz und Nachrichtendienste (DSN) wird erneut auf die Gefährdung durch ausländische Desinformationskampagnen hingewiesen. Hierbei zeigt sich, dass insbesondere seit dem Beginn des russischen Angriffskriegs russische „Trollnetzwerke“ in Österreich aktiv sind. Diese Netzwerke haben einen starken Einfluss auf die Szene der „Neuen-Rechten“, deren Akteure oft eine ausgeprägte Affinität zu Russland zeigen. (DSN 2025b, 31–32) Neben diesen Einflüssen von Desinformationskampagnen lassen sich auch Einflüsse auf den „Heterodoxen Extremismus“ beobachten. Diese Form des Extremismus lässt sich nicht klar dem links-extremen oder dem rechts-extremen Milieu zuordnen, sondern ist eine Mischung bestehend aus Covid-Maßnahmen-Gegner, Esoterikern, Sektenmitgliedern, Personen aus der staatsfeindlichen Szene und Impf- beziehungsweise Abtreibungsgegnern. Gemeinsam ist diesen Gruppen, dass sie an übergeordnete große Verschwörungen glauben, dass sie die demokratische und rechtstaatliche Grundordnung ablehnen und, dass sie an „Wir-gegen-Sie“ Erzählungen glauben. Elementarer Bestandteil des heterodoxen Extremismus ist der Glaube, dass verschiedene Verschwörungserzählungen wie die „Klimahysterie“, oder der „Große Austausch“ auf einer Meta-Verschwörungsebene zusammenhängen und von der angeblichen globalen Elite ausgenutzt werden, um die Menschen in ihren Rechten zu beschneiden. Des Weiteren sind antisemitische Narrative oft ein Bestandteil der Ideologie. (DSN 2025b, 42)

In Österreich sind Mitglieder dieser Gruppierungen oft durch pro-russische Desinformationskampagnen beeinflusst und von diesen manipuliert. Sie verbreiten diese Desinformation anschließend auf ihren eigenen Kanälen und Netzwerken, den sogenannten alternativen Medien, innerhalb von Österreich weiter. Somit unterstützen sie die FIMI-Bemühungen ausländischer Staaten. Ein besonders reichweitenstarkes alternatives Medium

ist der Online-TV Kanal „Auf1“, der regelmäßig Verschwörungstheorien, pro-russische Propaganda beziehungsweise Desinformation sowie demokratiefeindliche Inhalte verbreitet. Im September 2025 hat der deutsche Verfassungsschutz bekannt gegeben, dass „Auf 1“ als rechtsextremer Verdachtsfall eingestuft wird und nachrichtendienstlich beobachtet wird. (Sulzbacher 2025) Gemeinsam mit anderen alternativen Medien und einschlägigen Telegram-Gruppen entsteht somit eine Art Parallelgesellschaft. In Österreich sind diese Gruppierungen im internationalen Vergleich besonders mitgliederstark. Laut der „European Union Terrorism Situation and Trend Report 2023“ von EUROPOL existiert in Österreich nach Deutschland die europaweit zweitgrößte Szene. Aufgrund der gemeinsamen Sprache gibt es allerdings große Überschneidungen und gegenseitige Beeinflussung zwischen den jeweiligen Szenen. Insbesondere seit dem Ausbruch der Covid-19 Pandemie 2020 verzeichnet man ein starkes Wachstum der Szene. (DSN 2025b, 41–43)

Das österreichische Vereinswesen sowie dessen rechtliche Stellung ermöglichen es, durch verschachtelte Konstruktionen undurchsichtige Eigentümerstrukturen zu schaffen. Dies erschwert eine Überwachung der alternativen Medien durch die DSN und ein effektives Vorgehen der Behörden gegen die dort verbreitete Desinformation. Des Weiteren haben sich die alternativen Medien im Wahljahr 2024 als effektives Einfallstor und als bedeutender Kanal für ausländische Desinformation gezeigt. (DSN 2025b, 43) In den vergangenen Jahren hat sich in Österreich gezeigt, dass ausländische Gruppierungen mittels FIMI-Kampagnen versuchen verschiedene Diasporagruppen in Österreich zu beeinflussen. Somit werden bereits bestehende gesellschaftliche Spannungen und Spaltungen noch weiter vertieft. (DSN 2025b, 91–92) Im März 2025 ist durch die DSN eine FIMI-Zelle in Österreich ausgeforscht worden. Diese hat in Österreich Desinformationen zum Nachteil der Ukraine verbreitet. Die Auftraggeber dieser Gruppe befinden sich vermutlich in Russland. (DSN 2025a)

8.4.2 Das Konzept der umfassenden und der geistigen Landesverteidigung

In Österreich gibt es das Verteidigungskonzept der umfassenden Landesverteidigung, welches ähnlich wie in der Schweiz zur Zeit des Kalten Krieges entwickelt worden ist. Zur umfassenden Landesverteidigung gehören neben der militärischen Landesverteidigung auch die zivile, die wirtschaftliche und die geistige Landesverteidigung. Als strategische Erweiterung der

umfassenden Landesverteidigung ist es das Ziel der geistigen Landesverteidigung, die innere Widerstandfähigkeit der Gesellschaft gegen ausländische Propaganda und Beeinflussung zu stärken und somit auch die Resilienz gegen FIMI und Desinformationskampagnen zu stärken. Die Umfassende Landesverteidigung sowie die geistige Landesverteidigung sind in Österreich seit 1975 in Artikel 9a des Bundesverfassungsgesetzes festgeschrieben und somit auch Teil des Unterrichtsplans. (Bundesministerium für Bildung, o. J.)

(1) Österreich bekennt sich zur umfassenden Landesverteidigung. Ihre Aufgabe ist es, die Unabhängigkeit nach außen sowie die Unverletzlichkeit und Einheit des Bundesgebietes zu bewahren, insbesondere zur Aufrechterhaltung und Verteidigung der immerwährenden Neutralität. Hierbei sind auch die verfassungsmäßigen Einrichtungen und ihre Handlungsfähigkeit sowie die demokratischen Freiheiten der Einwohner vor gewaltsamen Angriffen von außen zu schützen und zu verteidigen. (Art. 9a B-VG)

(2) Zur umfassenden Landesverteidigung gehören die militärische, die geistige, die zivile und die wirtschaftliche Landesverteidigung. (Art. 9a B-VG)

Im Zusammenhang mit der Verteidigung gegen FIMI-Bedrohungen ist insbesondere das Konzept der geistigen Landesverteidigung relevant. Dieses Konzept besagt, dass es notwendig ist in der eigenen Bevölkerung das Bewusstsein für den Wert der Demokratie, der pluralistischen Gesellschaft, der nationalen Souveränität sowie der nationalen Identität durch die Verbesserung der Medienkompetenz, Bildung und die Vermittlung von gesellschaftlichen Werten zu steigern. Die geistige Landesverteidigung ist somit ein Instrument zur Entwicklung von Resilienzen gegen FIMI, das nicht nur rechtlich verankert ist, sondern dass auch durch die Einbindung in die Schulcurricula breitenwirksam die Bevölkerung erreicht. Zur Erfüllung dieser Aufgabe organisiert das Bundesministerium für Landesverteidigung in Kooperation mit dem Bildungsministerium das Informationsoffizierswesen. Hierbei werden so genannte Informationsoffiziere an Schulen eingeladen, um dort Vorträge und Schulungen über die Verbrechen während der NS-Zeit, die Demokratie, gesellschaftliche Werte, die Neutralität, die Aufgaben des Bundesheeres, die möglichen Bedrohungen für Österreich und die Verbreitung von Fehlinformation und Desinformation zu halten. (BMLV 2025)

Das Konzept der umfassenden Landesverteidigung und in diesem Fall auch das Konzept der geistigen Landesverteidigung weist somit auf den ersten Blick große Ähnlichkeiten zu den beiden schwedischen Konzepten der totalen Verteidigung und der psychologischen Verteidigung auf. Im Unterschied zu Schweden wird die geistige Landesverteidigung von den österreichischen Behörden allerdings anders umgesetzt. So gibt es zum Beispiel kein entsprechendes Gegenstück zur schwedischen psychologischen Verteidigungsagentur. Vielmehr stehen in der österreichischen geistigen Landesverteidigung das österreichische Bundesheer sowie die Aufrechterhaltung der Neutralität im Vordergrund. Mit der Einführung der österreichischen Sicherheitsstrategie im Jahr 2024 kann sich dies allerdings ändern.

8.4.3 Die österreichische Sicherheitsstrategie von 2024

Obwohl es in Österreich keine eigene Strategie zur Verteidigung von FIMI-Vorfällen gibt, bekennt man sich in der „Österreichischen Sicherheitsstrategie“ (ÖSS) aus dem Jahr 2024 dazu gegen hybride Bedrohungen, zu denen Desinformation und ausländische Einflussnahme zählen, Resilienzen aufzubauen und eine wirksame gesamtstaatliche strategische Kommunikationspolitik zu etablieren. Hierbei liegt Fokus darauf, Desinformation und Manipulation durch ausländische Staaten und deren Proxies im Zusammenhang mit dem Themenkomplex Migration und Asyl zu verhindern. (ÖSS 2024) Hierzu wird unter anderem folgendes festgehalten:

„Um die politische Instrumentalisierung von Migration durch autokratische Staaten oder nicht-staatliche Akteure zu verhindern, bedarf es vor allem weiterhin einer wirksamen gesamtstaatlichen strategischen Kommunikation. Dadurch soll auch gegen Desinformations- und Manipulationsversuche wirksam vorgegangen werden. Ein zukunftsweisender und verantwortlicher Diskurs über die Zusammenhänge von Migration, Gesellschaft, Demokratie und Rechtsstaat ist weiterhin in allen Bildungsbereichen zu gewährleisten.“ (ÖSS 2024, 29)

In der ÖSS wird Russland als der primäre Akteur bezeichnet, der versucht mit hybriden Mitteln die demokratischen Strukturen in Österreich und der EU zu schwächen und die europäischen Integrations- und Entscheidungsprozesse zu untergraben. Auch wenn russische FIMI-Vorfälle nicht explizit erwähnt werden, wird die Gefahr sowie ihr Urheber erkannt und klar benannt. Der österreichische Ansatz zur FIMI-Verteidigung unterscheidet sich von den anderen

untersuchten Ansätzen dadurch, dass in Österreich der religiöse Extremismus, insbesondere der radikale Islam oder auch politische Islam, eine wesentlich höher gewichtete Stellung einnimmt. (ÖSS 2024)

8.4.4 Die involvierten Behörden und NGOs

In Österreich übernehmen mehrere verschieden Ministerien und Ämter die Kompetenzen zur Abwehr von FIMI-Vorfällen. Involviert sind, das Bundesministerium für Inneres, das Bildungsministerium, das Bundeskanzleramt, die Direktion Staatsschutz und Nachrichtendienste (DSN), die dem Bundesministerium für Inneres zugehörig ist, das Verteidigungsministerium und das Außenministerium. Die Direktion Staatsschutz und Nachrichtendienst (DSN) ist für die Aufdeckung, Analyse und Abwehr von FIMI-Vorfällen im Inland zuständig, insbesondere wenn diese sicherheitsrelevante Strukturen betreffen. Das Bundeskanzleramt koordiniert die strategische Kommunikation der Bundesregierung, setzt EU-Initiativen gegen Desinformation um und betreibt Öffentlichkeitsarbeit zur Sensibilisierung. (BKA 2025b) Das Bildungsministerium fördert Medien- und Informationskompetenz im Rahmen der Schulbildung, unter anderem durch Lehrpläne und Projekte zur kritischen Informationsnutzung. Hierbei wird auch ein Fokus auf den kritischen Umgang mit KI gelegt. (BMB, o. J.) Das Außenministerium vertritt Österreich in der EU und in internationalen Gremien, koordiniert außenpolitische Beiträge zu FIMI-Themen und arbeitet mit Partnerstaaten zusammen. Hier übernimmt insbesondere die Abteilung II2 „Sicherheitspolitische Angelegenheiten“ die FIMI-Agenden. (BMEIA 2025) Im Rahmen der Lagebilderstellung für hybride Bedrohungen und bei der Bewertung von FIMI-Bedrohungen spielen das Verteidigungsministerium und das dazugehörende Abwehramt eine unterstützende Rolle.

Zur Förderung der Resilienz und der „digital Literacy“ existiert die Online-Plattform „Zentrum Polis“, über welche Lehrer Zugriff auf Lernunterlagen erhalten können, mit denen sie in ihrem Unterricht über die Gefahren von Desinformation aufklären können. Auf diese Plattform sind unter anderem Informationen über die russischen Narrative zum Ukrainekrieg oder verschiedene Sichtweisen zum Nahost-Konflikt zu finden. Neben Initiativen im Bildungsbereich gibt es noch weitere. So wird von der Parlamentsdirektion die „Demokratiewerkstatt“,

betrieben. Hierbei handelt es sich ebenfalls um eine Online-Plattform, auf der Informationen über Desinformation und Fake-News und deren Erkennung aufbereitet werden. Ähnliche Aufklärung bieten auch die WKO sowie die Plattform Jugendportal.at an. Neben der Aufklärung der eigenen Bevölkerung, bekennt sich Österreich auch zu einer gesamtstaatlichen strategischen Kommunikation. Hierfür gibt es verschiedene Fakten-Checker, die Desinformations- und FIMI-Vorfälle aufdecken und veröffentlichen, wie den APA-Fakten-Checker und den Verein Mimikama. (Bundeskanzleramt Österreich 2025) Zum momentanen Zeitpunkt gibt es keine eigenen restriktiven Maßnahmen zur Inhaltsmoderation, wie zum Beispiel ein Verbot bestimmter Kanäle oder Sender. Allerdings werden EU-Vorgaben, wie der DSA, in Österreich umgesetzt.

8.4.5 Conclusio Österreich

Die österreichische FIMI-Abwehr befindet sich im Vergleich zu anderen Staaten zum momentanen Zeitpunkt noch im Anfangsstadium. Es gibt noch keine eigene FIMI-Strategie und es fehlt zurzeit ebenso eine zentrale Steuerungsbehörde. Erste Schritte zur Schaffung einer zentralen FIMI-Behörde sind allerdings bereits gesetzt worden. So gibt es die im Bundeskanzleramt angesiedelte „Arbeitsgruppe hybride Bedrohungen“, die die Ressorts übergreifende Zusammenarbeit im Bereich der hybriden Bedrohungen und im Bereich der FIMI-Abwehr übernimmt. Ebenso gibt es im Bundeskanzleramt seit 2024 das Krisensicherheitsbüro, das im Rahmen des Bundeskrisensicherheitsgesetzes neu geschaffen worden ist. Diese Stelle soll für die Bundesregierung geeignete Strategien und Handlungsmöglichkeiten zur Steigerung der Resilienz kreieren. (BKA 2025a)

Der österreichische Weg der FIMI-Abwehr ist in erster Linie präventiv und kommunikativ und folgt damit den Empfehlungen des DSN. (DSN 2025b) Es sind daher wenige restriktive Maßnahmen vorhanden. Ebenso wie in Deutschland kann man den deutschsprachigen Ableger von RT, RT DE, nicht mehr empfangen, da diesem die Sendelizenz entzogen worden ist. Dies liegt allerdings nicht an den österreichischen Regeln und Verboten, sondern an Entscheidungen der EU. Generell lässt sich in Österreich beobachten, dass viele Policies und Strategien im Bereich der FIMI-Verteidigung in Zusammenarbeit mit der EU entstehen. So stützt sich ein wesentlicher Teil der Bemühungen auf den Digital Service Act.

9 Ergebnisse und Beitrag zur Fachdebatte

Zusammenfassend kann gesagt werden, dass die europäischen Länder auf die neu entstehende FIMI-Bedrohung reagieren. Insbesondere seit dem russischen Angriffskrieg und den damit einhergehenden hybriden Aktivitäten von Seiten Russlands haben die europäischen Staaten erkannt, dass zentrale europäische Werte wie Demokratie, Meinungsfreiheit und nationalstaatliche Souveränität nur aufrechterhalten werden können, wenn man versucht ausländische Einflussnahmen zu unterbinden und Schritte unternimmt, um die Widerstandsfähigkeit der eigenen Bevölkerung zu stärken. Bei diesen Bemühungen kooperieren die europäischen Staaten zunehmend miteinander und arbeiten eng mit den verschiedenen europäischen Institutionen zusammen. Insbesondere die Arbeit des EEAS, dessen Datensammlung sowie die FIMI-Toolbox werden von den Mitgliedstaaten als Entscheidungsgrundlage und Empfehlungen verwendet. (EEAS 2024a)

Deutschland, Frankreich und Österreich haben erst auf die FIMI-Bedrohung reagiert und politische Änderungen umgesetzt, als man die Auswirkungen von FIMI-Kampagnen in Europa bereits beobachten und spüren konnte. So hat man zum Beispiel in Frankreich die weitreichenden FIMI- und Desinformationsgesetze erst erlassen, als es im Jahr 2017 zu massiven FIMI-Kampagnen, die Russland zugeschrieben werden, im Rahmen der Präsidentschaftswahlen gekommen ist. (Bayer u. a. 2021) In Schweden hingegen ist man sich bereits während der Zeit des Kalten Kriegs der Bedrohung durch ausländische Propaganda und ausländische Beeinflussung bewusst geworden. Dementsprechend hat man bereits früh die ersten Maßnahmen zur Entwicklung der Widerstandsfähigkeit der Bürger umgesetzt und eigene Behörden wie die MPF und den MSB geschaffen. Inzwischen kann Schweden seine langjährigen Erfahrungen im Rahmen der EU-Institutionen an andere Länder in Form von „best-practice“ Beispielen weitergeben. (Pamment und Isakson 2024) In Deutschland und Österreich ist man sich den Bedrohungen durch ausländische Beeinflussung erst bewusst geworden, als im Zusammenhang mit dem Ukraine-Krieg ab 2022 massive russische FIMI-Kampagnen beobachtet worden sind und die beiden Länder mit einer neuen geopolitischen Situation konfrontiert gewesen sind. Als Reaktion hat Deutschland im Jahr 2023 die nationale Sicherheitsstrategie beschlossen und Österreich im Jahr 2024 die Österreichische Sicherheitsstrategie. In diesen Beiden Dokumenten werden FIMI und hybride Bedrohungen als

Sicherheitsrisiken identifizieren. (ÖSS 2024; NSS 2023) In beiden Ländern existiert zum momentanen Zeitpunkt, im Gegensatz zu Frankreich und Schweden, noch keine eigene FIMI- oder Desinformationsstrategie, jedoch wird das Thema in den neuen nationalen Sicherheitsstrategien behandelt.

Im organisatorischen Bereich zeichnet sich ab, dass in Frankreich und Schweden die Verteidigung gegen Desinformation und FIMI im Aufgabenbereich von eigens dafür eingerichteten Behörden und Ämtern zentral organisiert ist. In Deutschland und Österreich hingegen sind die Zuständigkeiten auf verschiedene Ministerien aufgeteilt und es besteht keine zentrale hauptverantwortliche Stelle. Sowohl die späte Entscheidung, eine staatliche FIMI-Abwehr zu etablieren, als auch die dezentrale und fragmentierte Struktur der FIMI-Abwehr lassen sich mit den Mechaniken der Pfadabhängigkeit innerhalb der Theorie des historischen Institutionalismus erklären. In Deutschland und in Österreich hat man in der Vergangenheit negative Erfahrungen mit staatlichen Eingriffen in die Meinungsbildung und der staatlichen Kontrolle von Information gemacht. Während der NS-Zeit, der DDR-Zeit und während des Austrofaschismus haben zentral gelenkte staatliche Behörden massiven Einfluss auf die öffentliche Meinung genommen. (Hallin und Mancini 2004) Geprägt durch diese negativen Erfahrungen ist es möglich, dass man in Deutschland und Österreich bei staatlicher Einflussnahme in die Medienfreiheit und Eingriffen in den öffentlichen Diskurs eher zurückhaltend agiert.

Ebenfalls kann man die Pfadabhängigkeit als Erklärungsansatz heranziehen, warum die Verantwortung für die FIMI-Abwehr in Österreich und Deutschland zwischen verschiedenen Ministerien und Ämtern aufgeteilt ist. In beiden Ländern schotten sich einzelne Verwaltungseinheiten gegenüber anderen Sektoren ab, agieren stark kompetenzorientiert und lehnen eine zentrale sowie übergeordnete Steuerung ab. (Derlien 2003; Fleischer 2021, 66–68) Insbesondere in einem ressortübergreifenden Politikfeld wie der FIMI-Abwehr, welches verschiedene politische Bereiche wie die Bildungspolitik, die Medienpolitik, die Sicherheitspolitik und die Außenpolitik betrifft, ist es für Staaten mit einer zentralistischen Verwaltung, wie sie etwa in Frankreich vorhanden ist, einfacher zentrale Entscheidungs- und Steuerungsstrukturen zu etablieren. Mit solchen zentralen Strukturen kann man schneller und

effektiver auf die sich schnell verändernde FIMI-Bedrohung reagieren und notwendige Anpassungen rascher vornehmen.

Die in Kapitel 3 vorgestellten Theorien zu Policy Veränderungen in Zeiten von Krisen und zu den Lerneffekten im Rahmen der OMK, lassen sich in einigen Punkten auch bei der Entstehung der von FIMI-Abwehr-Policies wiedererkennen. In diesem Bereich lassen sich europaweit seit 2015 verstärkte Zusammenarbeit und Koordination beobachten. Juncos et al. schreiben, dass Krisen vermehrte Kooperation auslösen können, wenn eine Krise alle Mitglieder in ähnlicher Art und Weise trifft. (Juncos u. a. 2025) Obwohl die EU-Mitglieder zu unterschiedlichen Zeitpunkten und unterschiedlich intensiv von russischen Desinformationskampagnen betroffen gewesen sind, hat die Mehrheit von ihnen erkannt, dass die einzelnen nationalen Krisen eine Krise für die gesamte EU darstellen können. Um die Handlungsfähigkeiten der EU in der Außen- und Verteidigungspolitik massiv einzuschränken, ist es ausreichend, wenn in einem Mitgliedsstaat eine russlandfreundliche Regierung die Regierungsverantwortung übernimmt und EU-Ratsbeschlüsse, die Einstimmigkeit erfordern, blockiert.

Auch wenn das FIMI-Problem neu ist und die Mitgliedsstaaten in ihrer ersten Reaktion auf die Bedrohung individuelle Strategien und Abwehrmaßnahmen eingeführt haben, zeigt sich inzwischen, dass es im Rahmen der europäischen Institutionen vermehrt zu Policy-Konvergenzen kommt. Hier sticht insbesondere die Ausarbeitung der FIMI-Toolbox hervor. Diese Methode bildet einen einheitlichen europäischen Maßnahmenkatalog ab und zeigt, dass sich Policy-Angleichungen auch im FIMI-Bereich erkennen lassen. (EEAS 2024a) Die Reaktion Frankreichs auf die FIMI-Vorfälle im Jahr 2017 zeigt allerdings auch, dass die initiale Reaktion und die initiale Policy-Veränderung zunächst auf der nationalen Ebene erfolgt und die Policies erst im Laufe der Zeit auf der europäischen Ebene vereinheitlicht werden. Hier hat sich zum Beispiel das RAS als zwischenstaatliche Austauschplattform im Sinne der OMK etabliert.

10 Weitere Entwicklung der europäischen FIMI-Abwehr und geopolitischer Ausblick

In den letzten Jahren sind einige der europäischen Staaten sowie die europäischen Institutionen, insbesondere der EEAS, zu Vorreitern in der Aufklärung und Analyse von FIMI-

Kampagnen geworden. Nationale und europäischen Strategiedokumente wie der europäische Kompass legen nahe, dass die gesamteuropäischen Fähigkeiten und Kapazitäten auch in den nächsten Jahren weiter ausgebaut werden. (European Union 2022) In vielen Bereichen ist man allerdings nach wie vor auf die Kooperation mit anderen Staaten angewiesen.

Entscheiden für die zukünftigen europäischen FIMI-Bemühungen und die internationale Kooperation im FIMI-Bereich wird neben den politischen Entscheidungen in Europa auch die weitere innenpolitische und außenpolitische Entwicklung der USA sein. Die zweite Amtszeit von Donald Trump könnte sowohl die Effektivität der amerikanischen FIMI-Abwehr nachhaltig beeinträchtigen als auch die transatlantische Zusammenarbeit mit europäischen Behörden und Geheimdiensten erschweren. Die zweite Amtszeit ist bislang geprägt von einem politisch motivierten Umbau der Verwaltung, gravierenden Budgetkürzungen, einer stetig steigenden Polarisierung der Bevölkerung und den Handels- und Zollstreitigkeiten mit anderen Staaten. Im FIMI-Bereich ist zum Beispiel die Finanzierung der amerikanische FIMI-Abwehrbehörde „global engagement center“ (GEC), die ein Vorreiter in der Aufdeckung von FIMI-Vorfällen gewesen ist, im Dezember 2024 ausgelaufen und von der republikanischen Mehrheit im Kongress nicht erneuert worden. Im April 2025 ist diese Behörde dann von Außenminister Marco Rubio mit der Begründung, dass diese Behörde rechte und konservative Stimmen zu Unrecht zensiere und somit die Meinungsfreiheit in den USA einschränken würde, komplett geschlossen worden. Ob es eine nachfolgende Behörde geben wird, ist noch nicht bekannt. (Politico 2025b) Man kann zum momentanen Zeitpunkt allerdings davon ausgehen, dass eine nachfolgende Behörde in ihren Handlungsmöglichkeiten wesentlich eingeschränkter wäre. Neben der GEC sind auch andere Behörden und Forschungseinrichtungen, die sich mit FIMI und Desinformation beschäftigt haben, von Budgetkürzungen und politisch motivierten Umstrukturierungen betroffen. (Scherling 2025) Diese Maßnahmen können die US-amerikanischen Fähigkeiten zur Erkennung und Bekämpfung von FIMI langfristig schwer beeinträchtigen. Aufgrund der engen Zusammenarbeit mit den europäischen NATO-Mitgliedern, hat eine Reduktion der amerikanischen Fähigkeiten und Kapazitäten einen direkten negativen Einfluss auf die europäischen Abwehrmöglichkeiten.

Des Weiteren kann die Rolle der amerikanischen Medien beim Fact-Checking von Desinformation und FIMI sowie bei der Aufklärung der Bevölkerung, durch Donald Trumps

regelmäßige Attacken gegen unabhängige Medien geschwächt werden. Angriffe, bei denen Medienunternehmen und Journalisten als Lügner oder wechselweise als Feinde der USA und des amerikanischen Volkes bezeichnet werden, können erstens dazu führen, dass das generelle Vertrauen der Bürger in die Medien abnimmt, wodurch deren aufklärende Wirkung abnimmt, und zweitens, dass die Medien, um den Angriffen zu entgehen, weniger Aufklärung über Desinformation und FIMI betreiben. Somit werden die Resilienz und die Medienkompetenz der amerikanischen Bevölkerung womöglich nachhaltig geschwächt. (Ross und Rivers 2018) Da europäische Bürger durch die global vernetzte Online-Welt auch der amerikanischen Medien- und Meinungssphäre ausgesetzt sind, kann eine Schwächung der Widerstandsfähigkeit in den USA die Verbreitung von FIMI auch in Europa erleichtern. Die US-amerikanische FIMI-Resilienz hat somit unmittelbare Auswirkungen auf den europäischen Meinungsraum und die europäischen Gegenstrategien. Zudem nutzen Russland und China gezielt aus, dass Trump selbst über diverse Kanäle viele Desinformationen und „Fake News“ verbreitet, indem sie seine Narrative und Lügen verstärken. So haben zum Beispiel russische, chinesische und iranische Akteure Trumps Narrativ, dass der „tiefe Staat“ sowie die Demokratische Partei angeblich für den gescheiterten Attentatsversuch auf seine Person verantwortlich sei, übernommen und dieses Narrative zur Verbreitung von Desinformationen genutzt. (Jingnan 2024)

Auch Donald Trumps Haltung zur EU und zur NATO inklusive der Zollstreitigkeiten, kann einen negative Einfluss auf die FIMI-Abwehr haben. So kann der US-Präsident unter anderem veranlassen, dass die amerikanischen Geheimdienste nicht mehr länger mit ihren transatlantischen Partnern zusammenarbeiten. Dies würde die Arbeit der europäischen Geheimdienste und die Arbeit des EEAS massiv erschweren. Donald Trump ist auch kein großer Befürworter der transatlantischen Zusammenarbeit und hat dies in der Vergangenheit auch immer wieder durch Kritik an der NATO und den europäischen Bündnispartner gezeigt. Neben diesen Problemen ist es auch möglich, dass im Rahmen der Zollverhandlungen mit der EU gefordert wird, den DSA oder den DMA zu verändern oder aufzuheben. Im Rahmen der Zollverhandlungen wird dies auch immer wieder von Seiten der USA gefordert. (der Standard 2025) Auch wenn diese beiden europäischen Verordnung unabhängig von den USA konzipiert und eingeführt worden sind, hat Donald Trump die europäischen Regulierungen mehrfach als

anti-amerikanisch und für die USA wirtschaftsschädigend kritisiert. Da die meisten von den beiden Verordnungen betroffenen Onlineplattformen US-amerikanischen Unternehmen gehören, läge ein Aufweichen der Verordnungen im wirtschaftlichen Interesse der USA. (Windwehr 2025) Sollte sich die amerikanische Regierung mit ihren Forderungen durchsetzen, hätte dies gravierende Auswirkungen auf die Regulierung von Online-Plattformen und somit auch auf das Entfernen von FIMI-Inhalten und die Verbreitung von Desinformation. Allerdings hat im März 2025 Henna Virkkunen, die EU-Kommissarin für Digitale- und Grenztechnologien, bestätigt, dass die europäischen Regulierungen von digitalen Technologien kein Teil der Verhandlungen mit den USA seien. Die Regulierung digitaler Unternehmen im EU-Raum habe europäischen Werten und Richtlinien zu folgen und sei daher kein Teil der transatlantischen Handelsbeziehungen und -verhandlungen. (Politico 2025a) Des Weiteren würde ein Nachgeben gegenüber den US-Forderungen einen Prestige- und Souveränitätsverlust für die EU-Kommission bedeuten. Daher kann man zum momentanen Zeitpunkt nicht davon ausgehen, dass sich die Trump-Regierung mit ihren Forderungen bezüglich DSA und DMA durchsetzen kann.

In Kombination dieser Faktoren kann also die politische Entwicklung in den USA dazu führen, dass sich die europäischen Staaten Abwehr-Kompetenzen vermehrt selbst aneignen müssen und, dass man sich, insbesondere im geheimdienstlichen Bereich, nicht mehr auf die transatlantische Achse und den gegenseitigen Informationsaustausch verlassen kann. Auch die Umsetzung digitaler Regulierung sowie die Weiterentwicklung der bestehenden Verordnungen wird gegen den Widerstand der US-Regierung schwerer zu erreichen sein. Für Europa ist es daher wichtig, die bestehenden transatlantischen Beziehungen sowie die Möglichkeiten zur Regulierung von digitalen Technologien in Form des DSA und des DMA zu bewahren. Eventuell lassen sich politische Kompromisse finden, indem man den USA und Donald Trump in anderen Politikbereichen entgegenkommt. Eine Möglichkeit hierfür wäre es die Verteidigungsausgaben zu erhöhen.

Von den politischen Entwicklungen in den USA unabhängig, muss die FIMI-Abwehr in Europa weiterentwickelt und gestärkt werden. Russland und China werden ihre FIMI-Operationen fortsetzen und neue, effektivere und schwerer erkennbare Methoden zur Beeinflussung entwickeln. Andere autokratische Staaten beobachten die bisherigen Erfolge von FIMI-

Operationen sowie deren Kosteneffizienz und könnten dadurch ebenso erwägen, diese Art der hybriden Kriegsführung zum Erreichen ihrer strategischen Interessen und Ziele zu nutzen. Die europäischen Staaten werden daher, mit Unterstützung der EU und des EEAS, weiterhin ihre FIMI-Strategien und ihre Abwehr-Policies verbessern und weiterentwickeln müssen. Sie sollten ebenso weiterhin ihre Kapazitäten zur Erkennung und Analyse von FIMI und Desinformation stärken. Diese Verbesserung der Verteidigungskapazitäten muss vor dem Hintergrund geschehen, dass bereits zum momentanen Zeitpunkt mittels FIMI-Kampagnen, wie jener während der rumänischen Präsidentschaftswahl 2024, versucht wird, öffentlichen Meinungen in den Mitgliedsstaaten zu beeinflussen. (McGrath und Dumitrache 2025) Somit werden bereits jetzt die fundamentalen Werte sowie die Souveränität der Mitgliedsstaaten in Frage gestellt und untergraben. Dies kann die Verteidigungsfähigkeit der EU-Mitglieder in Zukunft untergraben.

11 Literaturverzeichnis

Authoritarian Interference Tracker, Nick. 2025. „Authoritarian Interference Tracker“. Alliance For Securing Democracy - German Marshall Fund. https://securingdemocracy.gmfus.org/toolbox/authoritarian-interference-tracker/.

Banks, William C. 2019. *The Bumpy Road to a Meaningful International Law of Cyber Attribution*. 113 (Jänner): 191–96. https://doi.org/10.1017/aju.2019.32.

Bayer, Judit. 2024. „The EU policy on disinformation: aims and legal basis“. *Journal of Media Law* 16 (1): 18–27. https://doi.org/10.1080/17577632.2024.2362478.

Bayer, Judit, Natalija Bitiukova, Petra Bard, Judit Szakács, Alberto Alemanno, und Erik Uszkiewicz. 2019. „Disinformation and Propaganda – Impact on the Functioning of the Rule of Law in the EU and Its Member States“. SSRN Scholarly Paper 3409279. Social Science Research Network, Februar 1. https://doi.org/10.2139/ssrn.3409279.

Bayer, Judit, Bernd Holznagel, Katarzyna Lubianiec, u. a. 2021. „Disinformation and Propaganda: Impact on the Functioning of the Rule of Law and Democratic Processes in the EU and Its Member States - 2021 Update“. *European Parliament, Directorate-General for External Policies*, advance online publication. https://doi.org/doi:10.2861/752863.

Bechis, Francesco. 2020. „Playing The Russian Disinformation Game: Information operations from Soviet tactics to Putin’s sharp power“. In *Democracy and Fake News*. Routledge.

Benkler, Yochai, Robert Faris, und Harold Roberts. 2018. *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*. Oxford University Press.

Benkler, Yochai, Robert Farris, und Hal Roberts. 2018. *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*. 1. Aufl. Oxford University Press. https://doi.org/10.1093/oso/9780190923624.001.0001.

Benthem, Tsvetelina, Talita Dias, und Duncan Hollis. 2022. „Information Operations under International Law“. *Vanderbilt Journal of Transnational Law* 55 (5): 1217.

Berger, Cathleen, und Charlotte Freihse. 2024. „Super Election Year 2024: A Super Year for Disinformation?“ *Upgrade Democracy*, Dezember 17. https://upgradedemocracy.de/en/superwahljahr-2024-superjahr-desinformation/.

Bergmanis-Korāts, Gundars, Tetiana Haiduchyk, Jakub Kubs, Marat Khusnutdinov, Fabio Belafatti, und Andrius Šuminas. 2025. „Impact of the Digital Services Act: A Facebook Case Study“. *NATO Strategic Communications Centre of Excellence* (Riga), Mai 9.

BKA. 2025a. „Erstes Gesamtstaatliches Lagebild Österreichs veröffentlicht - Bundeskanzleramt Österreich“. Bundeskanzleramt Österreich, Juli 25. https://www.bundeskanzleramt.gv.at/themen/krisensicherheitsbuero/nachrichten-

des-krisensicherheitsbueros/erstes-gesamtstaatliches-lagebild-oesterreichs-veroeffentlicht.html.

BKA. 2025b. „Kampf gegen Desinformation - Bundeskanzleramt Österreich“. Bundeskanzleramt Österreich. https://www.bundeskanzleramt.gv.at/themen/kampf-gegen-desinformation.html.

Blatter, Joachim, und Markus Haverland. 2012. *Designing case studies: Explanatory approaches in small-N research*. Springer. https://books.google.com/books?hl=de&lr=&id=mcpfAQAAQBAJ&oi=fnd&pg=PP1&dq=Blatter,+Joachim%3B+Haverland,+Markus+(2012)&ots=AN_PxUXJK9&sig=0sn_Ie-4sogDopCwEfFFK9LAZwQ.

Bleyer-Simon, Konrad. 2025. „Policy Paper: Addressing Foreign Information Manipulation in the Context of European Regulations“. *Institute of Communication Studies*, Juni 10. https://iks.edu.mk/en/research-analysis/policy-paper-addressing-foreign-information-manipulation-in-the-context-of-european-regulations/.

BMB. o. J. „Digitale/mediale Kompetenzen“. Bildungsministerium. Zugegriffen 13. August 2025. https://www.bmb.gv.at/Themen/oesterr_jugendstrategie/digi_media.html.

BMEIA. 2025. „Geschäftseinteilung BMEIA“. Außenministerium Österreich. https://www.bmeia.gv.at/ministerium/geschaeftseinteilung/abteilung-ii2?.com.

BMI. 2025. „Maßnahmen der Bundesregierung gegen Desinformation“. Bundesministerium des Innern und für Heimat. https://www.bmi.bund.de/SharedDocs/schwerpunkte/DE/desinformation/massnahmen-der-bundesregierung.html?nn=21255176.

BMJ. 2022. „Digital Services Act“. Bundesministerium für Justiz. https://www.bmvrdj.gv.at/themen/EU-und-Internationales/Digital-Services-Act.html.

BMLV. 2025. „Service für Schulen“. Bundesheer.at. https://www.bundesheer.at/service/service-fuer-schulen.

Bradshaw, Samantha, und Philip N Howard. 2020. „Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation“. *University of Oxford*.

Bridgman, Aengus, Ferdinand Gehringer, Taylor Owen, und Alexander Romanishyn. 2024. „Countering Foreign Information Manipulation and Interference Lessons from the 2024 European Elections“. *Konrad Adenauer Stiftung*.

Bundesamt für Verfassungsschutz. 2023. „Desinformation als Mittel gezielter Einflussnahme fremder Staaten“. Bundesamt für Verfassungsschutz - Spionage- und Proliferationsabwehr -. https://www.verfassungsschutz.de/SharedDocs/hintergruende/DE/spionage-und-proliferationsabwehr/desinformation.html.

Bundeskanzleramt Österreich. 2025. „Kampf gegen Desinformation - Bundeskanzleramt Österreich“. Bundeskanzleramt Österreich. https://www.bundeskanzleramt.gv.at/themen/kampf-gegen-desinformation.html.

Bundesministerium für Bildung. o. J. „Geistige Landesverteidigung“. Zugegriffen 12. August 2025. https://www.bmb.gv.at/Themen/schule/schulpraxis/ba/glv.html.

Bundestag. 2025. *Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Konstantin Kuhle, Renata Alt, Christine Aschenberg-Dugnus, weiterer Abgeordneter und der Fraktion der FDP – Drucksache 20/14166 –*. Bundestag. https://dserver.bundestag.de/btd/20/145/2014595.pdf.

Cenusa, Denis. 2024. „Countering Russian Hybrid Interference with EU Sanctions“. *Geopolitics and Security Studies Center, GSSC (Previously Known as Eastern Europe Studies Centre, EESC)*. https://www.gssc.lt/en/publication/countering-russian-hybrid-interference-with-eu-sanctions/.

Chechelashvili, Maia, Lia Berikashvili, und Elisabed Malania. 2020. „Foreign Interference in Electoral Processes as a Factor of International Politics: Mechanisms and Counteraction“. *Foreign Affairs*, Nr. 33: 33(6). https://doi.org/10.46493/2663-2675.33(6).2023.52-62.

Chłoń, Tomasz, Robert Kupiecki, und Filip Bryjka. 2024. *International Disinformation*. Brill. https://brill.com/display/title/71367.

Couzigou, Irène. 2021. „The French Legislation Against Digital Information Manipulation in Electoral Campaigns: A Scope Limited by Freedom of Expression“. *Election Law Journal* 20 (1): 98–115. https://doi.org/10.1089/elj.2021.0001.

D’Andrea, Alessia, Giorgia Fusacchia, und Arianna D’Ulizia. 2025. „Policy Review: Countering Disinformation in the Digital Age - Policies and Initiatives to Safeguard Democracy in Europe“. *Information Polity*, März 19, 15701255251318900. https://doi.org/10.1177/15701255251318900.

David, Samantha. 2022. „Votes, Budgets, Rules: How the French Election Works and Quirky Facts“. The Connexion, April 6. https://www.connexionfrance.com/practical/votes-budgets-rules-how-the-french-election-works-and-quirky-facts/176742.

Davituliani, Salome. 2024. „THE NEXUS OF DISINFORMATION, ATTRIBUTION, AND ESCALATION: UNRAVELING THE COMPLEXITIES OF CYBER OPERATIONS AND WARFARE“. თავდაცვა და მეცნიერება 3 (Dezember): 57–63. https://doi.org/10.61446/ds.3.2024.8473.

der Standard. 2025. „Streit über Digitalgesetze verzögert Handelsabkommen von EU und USA“. DER STANDARD, August 17. https://www.derstandard.at/story/3000000283709/streit-ueber-digitalgesetze-verzoegert-handelsabkommen-von-eu-und-usa.

Derlien, Hans-Ulrich. 2003. „German Public Administration: Weberian Despite ‚Modernization'". *Universität Bamberg - Lehrstuhl Für Verwaltungswissenschaft - Veröffentlichungen*, Universität Bamberg - Lehrstuhl für Verwaltungswissenschaft - Veröffentlichungento be published in: Krishna K. Tummala (ed.), Comparative Bureaucracy, Aufsatz (2003).

Dias, Talita. 2023. „Study international norms on FIMI". *European Union External Action Service*. https://www.eeas.europa.eu/sites/default/files/documents/2024/Study%20international%20norms%20on%20FIMI.pdf.

Dowling, Melissa-Ellen. 2021. „Democracy under Siege: Foreign Interference in a Digital Era". *Australian Journal of International Affairs* 75 (4): 383–87. https://doi.org/10.1080/10357718.2021.1909534.

Dragomir, Marius, José Rúas-Araújo, und Minna Horowitz. 2024. „Beyond Online Disinformation: Assessing National Information Resilience in Four European Countries". *Humanities and Social Sciences Communications* 11 (1): 101. https://doi.org/10.1057/s41599-024-02605-5.

Drolsbach, Chiara Patricia, Kirill Solovev, und Nicolas Pröllochs. 2024. „Community notes increase trust in fact-checking on social media". *PNAS Nexus* 3 (7): pgae217. https://doi.org/10.1093/pnasnexus/pgae217.

DSN. 2025a. „DSN deckt russische Desinformationskampagne gegen Ukraine auf". Dirketion Staatsschutz und Nachrichtendienste. https://www.dsn.gv.at/news.aspx?id=684974546579734E4A61453D.

DSN. 2025b. *Verfassungsschutzbericht 2024*. Direktion Staatsschutz und Nachrichtendienst.

EEAS. 2023. *Towards a framework for networked defence*. 1st. EEAS Report on Foreign Information Manipulation and Interference Threats. European External Action Service. https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023..pdf.

EEAS. 2024a. *A Framework for Networked Defence*. 2nd. EEAS Report on Foreign Information Manipulation and Interference Threats. European External Action Service. https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report%20on%20FIMI%20Threats-January-2024_0.pdf.

EEAS. 2024b. „Tackling Disinformation, Foreign Information Manipulation & Interference | EEAS". https://www.eeas.europa.eu/eeas/tackling-disinformation-foreign-information-manipulation-interference_en.

EEAS. 2025. *Exposing the Architecture of FIMI Operations*. 3rd. EEAS Report on Foreign Information Manipulation and Interference Threats. European External Action Service.

Europäischer Rat. 2019. „Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats“. European Council - Council of the European Union. https://www.consilium.europa.eu/en/council-eu/preparatory-bodies/horizontal-working-party-on-enhancing-resilience-and-countering-hybrid-threats.com.

European Council. 2024. „Russia: New Sanctions Framework against Those Responsible for Destabilising Activities against the EU and Its Member States“. Consilium. https://www.consilium.europa.eu/en/press/press-releases/2024/10/08/russia-eu-sets-up-new-framework-for-restrictive-measures-against-those-responsible-for-destabilising-activities-against-the-eu-and-its-member-states.com.

European Union. 2022. *EU Strategic Compass for security and defence*. European Union Strategic Communications. https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf.

European Union Agency for Cybersecurity. 2022. *Foreign Information Manipulation and Interference (FIMI) and Cybersecurity: Threat Landscape.* Publications Office. https://data.europa.eu/doi/10.2824/7501.

EUvsDisinfo. 2017. „COMMENTARY: Means, Goals and Consequences of the pro-Kremlin Disinformation Campaign“. EUvsDisinfo. https://euvsdisinfo.eu/commentary-means-goals-and-consequences-of-the-pro-kremlin-disinformation-campaign/.

EUvsDisinfo. 2025. „What We Have Learnt about FIMI after Three Years of Full-Scale War in Ukraine“. EUvsDisinfo, März 12. https://euvsdisinfo.eu/what-we-have-learnt-about-fimi-after-three-years-of-full-scale-war-in-ukraine/.

Ferrara, Federico Maria, und Hanspeter Kriesi. 2022. „Crisis Pressures and European Integration“. *Journal of European Public Policy* (London) 29 (9): 1351–73. https://doi.org/10.1080/13501763.2021.1966079.

Fleischer, Julia. 2021. „Federal Administration“. In *Public Administration in Germany*, herausgegeben von Sabine Kuhlmann, Isabella Proeller, Dieter Schimanke, und Jan Ziekow. Governance and Public Management. Springer International Publishing. https://doi.org/10.1007/978-3-030-53697-8.

Fridman, Ofer. 2024. „Defining Foreign Influence and Interference“. *INSS Special Publication*, Jänner 4, 1–12.

Fridman, Ofer, und Jean-Christopher Boucher. 2024. „Counter-FIMI-Toolbox.pdf“. Community of Democrats. https://community-democracies.org/app/uploads/2025/01/Counter-FIMI-Toolbox.pdf.

Galante, Laura, und Shaun Ee. 2018. „Defining Russian election interference: An analysis of select 2014 to 2018 cyber enabled incidents“. Atlantic council - Sowcroft center for Strategy and Security. https://www.atlanticcouncil.org/in-depth-research-

reports/issue-brief/defining-russian-election-interference-an-analysis-of-select-2014-to-2018-cyber-enabled-incidents-2/.

Giandomenico, Jessica, und Hanna Linderstål. 2025. *Disinfo landscape in Sweden V2*. Disinfo Lab. https://www.disinfo.eu/wp-content/uploads/2025/04/20250402_Disinfo-landscape-in-Sweden-V2.pdf.

Girardi, Benedetta, Timur Ghirotto, Laura Jasper, und Davis Ellison. 2025. *Scoping the threats: FIMI operations in the Indo-Pacific and Europe*. FIMI in Focus: Hague Centre for Strategic Studies. https://www.jstor.org/stable/resrep71344.4.

Gonçalves, João, Ina Weber, Gina M. Masullo, Marisa Torres Da Silva, und Joep Hofhuis. 2023. „Common Sense or Censorship: How Algorithmic Moderators and Message Type Influence Perceptions of Online Content Deletion". *New Media & Society* 25 (10): 2595–617. https://doi.org/10.1177/14614448211032310.

Guégan, Jean-Baptiste. 2024. „Paris 2024 : géopolitique des Jeux olympiques". *Politique étrangère* 242 (2): 157–69. https://doi.org/10.3917/pe.242.0157.

Guillaume, Marine. 2019. „Combating the Manipulation of Information – a French Case". *Hybrid CoE Strategic Analysis*, Nr. 16.

Hall, Peter A., und Rosemary C. R. Taylor. 1996. „Political Science and the Three New Institutionalisms". *Political Studies* 44 (5): 936–57. https://doi.org/10.1111/j.1467-9248.1996.tb00343.x.

Hallin, Daniel C., und Paolo Mancini. 2004. *Comparing Media Systems: Three Models of Media and Politics*. Communication, Society and Politics. Cambridge University Press. https://doi.org/10.1017/CBO9780511790867.

Hjortdal, Magnus. 2011. „China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence". *Journal of Strategic Security* 4 (2): 1–24.

Howard, Philip N. 2020. *Lie Machines : How to Save Democracy From Troll Armies, Deceitful Robots, Junk News Operations, and Political Operatives*. Yale University Press.

Humprecht, Edda, Frank Esser, und Peter Van Aelst. 2020. „Resilience to Online Disinformation: A Framework for Cross-National Comparative Research". *The International Journal of Press/Politics* 25 (3): 493–516. https://doi.org/10.1177/1940161219900126.

Hung, Tzu-Chieh, und Tzu-Wei Hung. 2022. „How China's Cognitive Warfare Works: A Frontline Perspective of Taiwan's Anti-Disinformation Wars". *Journal of Global Security Studies* 7 (4): ogac016. https://doi.org/10.1093/jogss/ogac016.

ICRC. 1949. *Genfer Konvention zum Schutz von Zivilpersonen in Kriegszeiten vom 12. August 1949*. Internationale Komitees vom Roten Kreuz.

ICRC. 2019. *icrc_ihl-and-cyber-operations-during-armed-conflicts*. Internationales Rotes Kreuz. https://www.icrc.org/sites/default/files/document/file_list/icrc_ihl-and-cyber-operations-during-armed-conflicts.pdf.

ICRC. 2022. „Cyberspace Is Not a Legal Vacuum, Including during Armed Conflict | ICRC". Dezember 12. https://www.icrc.org/en/document/cyberspace-not-legal-vacuum-including-during-armed-conflict.

Intelligence Online. 2023. „France : French Foreign Ministry to Set up 24/7 Disinformation Watch - 21/12/2023". Intelligence Online, Dezember 21. https://www.intelligenceonline.com/government-intelligence/2023/12/21/french-foreign-ministry-to-set-up-24_7-disinformation-watch,110131461-art.

Iso-Markku, Tuomas, und Niklas Helwig. 2024. „The Niinistö Report on Preparedness: Finland's Lessons for the EU and Their Limitations". *Finish Institute for International Affairs*, 9.

Janda, Jakub, Veronika Víchová, Monika Richter, Ilyas Sharibzhanov, und Jakub Fišer. 2017. „Overview of countermeasures by the EU28 to the Kremlin's subversion operations". *European Values*. https://europeanvalues.cz/wp-content/uploads/2022/04/overview-of-countermeasures-by-the-eu28-to-the-kremlin-s-subversion-operations.pdf.

Jansen, Nora. 2024. „The Ability of the Digital Services Act (DSA) to Fight Disinformation". SSRN Scholarly Paper 5076281. Social Science Research Network, November 29. https://doi.org/10.2139/ssrn.5076281.

Jingnan, Huo. 2024. „Foreign Influence Efforts Reached a Fever Pitch during the 2024 Elections". 2024 Election: Trump Wins 2nd Term as President. *NPR*, November 12. https://www.npr.org/2024/11/09/nx-s1-5181965/2024-election-foreign-influence-russia-china-iran.

Juncos, Ana E., Marianna Lovato, und Karolina Pomorska. 2025. „Coordinative Europeanization and Russia's War of Aggression: How Crises Shape Europeanization Dynamics in EU Foreign Policy". *Comparative European Politics* 23 (1): 118–38. https://doi.org/10.1057/s41295-024-00390-8.

Kachelmann, Matthias, und Wulf Reiners. 2023. „The European Union's Governance Approach to Tackling Disinformation – Protection of Democracy, Foreign Influence, and the Quest for Digital Sovereignty". *L'Europe En Formation* 396 (1): 11–36. https://doi.org/10.3917/eufor.396.0011.

Kaim, Markus, und Ronja Kempin. 2022. „Kompass oder Windspiel? Eine Analyse des Entwurfs für den »Strategischen Kompass« der EU". *SWP-Aktuell*, Stiftung Wissenschaft und Politik, A (01). https://doi.org/10.18449/2022A01.

Kaye, David, UN. Human Rights Council. Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, und UN. Human Rights Council. Secretariat, Hrsg. 2019. *Report of the Special Rapporteur on the Promotion and*

Protection of the Right to Freedom of Opinion and Expression: note. UN. https://digitallibrary.un.org/record/1631686.

Kozyreva, Anastasia, Stefan M. Herzog, Stephan Lewandowsky, u. a. 2023. „Resolving Content Moderation Dilemmas between Free Speech and Harmful Misinformation". *Proceedings of the National Academy of Sciences* 120 (7): e2210666120. https://doi.org/10.1073/pnas.2210666120.

Lahmann, Henning. 2020. „Information Operations and the Question of Illegitimate Interference under International Law". *Israel Law Review* 53 (2): 189–224. https://doi.org/10.1017/S0021223720000060.

Lehne, Stefan. 2022. *The EU and the Creative and Destructive Impact of Crises*. Oktober 18. https://policycommons.net/artifacts/3075992/the-eu-and-the-creative-and-destructive-impact-of-crises/3878300/.

Mahoney, James, und Kathleen Thelen, Hrsg. 2009. „A Theory of Gradual Institutional Change". In *Explaining Institutional Change: Ambiguity, Agency, and Power*. Cambridge University Press. https://doi.org/10.1017/CBO9780511806414.003.

Mansted, Katherine. 2021. *The Domestic Security Greyzone: Navigating the Space Between Foreign Influence and Foreign Interference*. https://nsc.anu.edu.au/sites/default/files/2024-06/Print_NSC_Foreign%20Interference_OP_2021.pdf.

Martin, Brian, und Sue Cury Jansen. 2015. „The Streisand Effect and Censorship Backfire". *International Journal of Communication* 9 (1): 0.

Mayring, Philipp, und Thomas Fenzl. 2019. „Qualitative Inhaltsanalyse". In *Handbuch Methoden der empirischen Sozialforschung*, herausgegeben von Nina Baur und Jörg Blasius. Springer Fachmedien. https://doi.org/10.1007/978-3-658-21308-4_42.

McGrath, Stephen, und Nicolae Dumitrache. 2025. „Romanians Confront a Deluge of Online Disinformation Ahead of a Presidential Election Rerun". AP News, April 27. https://apnews.com/article/romania-european-union-elections-disinformation-2cae1b28b5059b7cee228142eadaca78.

Meredith, Sam. 2018. „Facebook-Cambridge Analytica: A Timeline of the Data Hijacking Scandal". CNBC, April 10. https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html.

Müller, Patrick, und Peter Slominski. 2024. „Hungary, the EU and Russia's war against Ukraine: the changing dynamics of EU foreign policymaking". In *The War Against Ukraine and the EU: Facing New Realities*, herausgegeben von Claudia Wiesner und Michéle Knodt. Springer Nature Switzerland Cham. https://library.oapen.org/bitstream/handle/20.500.12657/90408/978-3-031-35040-5.pdf?sequence=1#page=119.

Nehring, Christopher. 2023. „Countering Disinformation - An evaluation of the institutional approach of governments“. *Institute for Global analytics* Briefing paper (4). https://www.academia.edu/download/111283152/Paper_4_Counter_Disinformation_Agencies.pdf.

Niinistö, Sauli. 2024. „Strengthening Europe’s Civilian and Military Preparedness and Readiness“. *Europäische Kommission*.

NSS. 2023. „Nationale Sicherheitsstrategie: Wehrhaft. Resilient. Nachhaltig. Integrierte Sicherheit für Deutschland“. https://www.bmvg.de/de/aktuelles/bundesregierung-beschliesst-erste-nationale-sicherheitsstrategie-5636234.

Ohlin, Jens David, Hrsg. 2020. „Limits of the Sovereignty Framework“. In *Election Interference: International Law and the Future of Democracy*. Cambridge University Press. https://doi.org/10.1017/9781108859561.004.

ÖSS. 2024. „Österreichische Sicherheitsstrategie 2024“. Bundeskanzleramt.

O’Sullivan, Donnie, Curt Devine, und Allison Gordon. 2023. „China is using the world’s largest online disinformation operation to harass Americans | CNN“. CNN. https://edition.cnn.com/2023/11/13/us/china-online-disinformation-invs/index.html.

Pamment, James. 2020a. *The EU’s Role in Fighting Disinformation: Developing Policy Interventions for the 2020s*. Carnegie Endowment for International Peace. https://carnegieendowment.org/files/Pamment_-_Regulation.pdf.

Pamment, James. 2020b. *The EU’s role in fighting disinformation: taking back the initiative*. https://carnegieendowment.org/files/Pamment_-_Future_Threats.pdf.

Pamment, James, und Elsa Isakson. 2024. *Psychological Defence: Concepts and principles for the 2020s*. text 6. MPF Report Series. Psycholgical Defence Agency. https://mpf.se/publikationer/publikationer/2024-10-28-psychological-defence-concepts-and-principles-for-the-2020s.

Persily, Nathaniel, und Joshua A. Tucker, Hrsg. 2020. *Social Media and Democracy: The State of the Field, Prospects for Reform*. 1. Aufl. Cambridge University Press. https://doi.org/10.1017/9781108890960.

Pichler, Dietmar. 2024. „Disinformation and Foreign Interference: A Challenge for the EU and Its Member States“. *Österreichische Gesellschaft Für Europapolitik*, Juni 6. https://www.oegfe.at/policy-briefs/disinformation-and-foreign-interference-a-challenge-for-the-eu-and-its-member-states/?lang=en.

Pierson, Paul. 2000. „Increasing Returns, Path Dependence, and the Study of Politics“. *American Political Science Review* 94 (2): 251–67. https://doi.org/10.2307/2586011.

Politico. 2025a. „EU social media law isn't censorship, tech chief tells US critic". https://www.politico.eu/article/social-media-law-does-not-regulate-speech-eu-tech-chief-tells-us-lawmaker-henna-virkkunen/.

Politico. 2025b. „State Department eliminates key office tasked with fighting foreign disinformation". POLITICO, April 16. https://www.politico.com/news/2025/04/16/state-department-shutters-gec-foreign-disinformation-00292982.

Potter, Nicholas. 2024. „RT-nahes Medium ‚Red': Hybrider Krieg in Berlin". *Die Tageszeitung: taz*, Oktober 12. https://taz.de/RT-nahes-Medium-Red/!6039623/.

Proto, Lucas, Paula Lamoso-González, und Luis Bouza Garcia. 2025. „The EU's FIMI Turn: How the European Union External Action Service Reframed the Disinformation Fight". *Media and Communication* 13. https://doi.org/10.17645/mac.9474.

Prysiazhniuk, Marianna. 2025. „Strategic Narratives and Information Warfare: Russian FIMI Campaigns against Ukraine's Armed Forces in the Context of War and Societal Impact". *Culture. Society. Economy. Politics* 5 (1): 88–108. https://doi.org/10.2478/csep-2025-0007.

Przeworski, Adam, und Henry Theune. 1970. *The Logic of Comparative Social Inquiry*. American Political Science Association. Wiley-Interscience. https://www.researchgate.net/publication/235413195_The_Logic_of_Comparative_Social_Inquiry.

Psychological defence Agency. 2025. „Psychological Defence Agency". Text. Februar 18. https://mpf.se/psychological-defence-agency.

Radaelli, Claudio M. 2003. *The Open Method of Coordination: A new governance architecture for the European Union?* Swedish Institute for European Policy Studies. https://ore.exeter.ac.uk/repository/bitstream/handle/10036/22489/Radaelli%20open%20Method.pdf?sequence=2.

Reporters without borders. 2025. „Index | RSF". Reporters without Borders. https://rsf.org/en/index.

Ross, Andrew S., und Damian J. Rivers. 2018. „Discursive Deflection: Accusation of "Fake News" and the Spread of Mis- and Disinformation in the Tweets of President Trump". *Social Media + Society* 4 (2): 2056305118776010. https://doi.org/10.1177/2056305118776010.

Rossbach, Niklas. 2017. *Strategic Outlook 7 - Perspectives on National Security in a New Security Environment*. Herausgegeben von Cecilia Hull Wiklund, Daniel Faria, Bengt Johansson, und Josefin Öhrn-Lundin. The Swedish Defense Research Agency.

Salzen, Claudia von. 2015. „Die EU und russische Desinformation: Eine Task Force gegen Propaganda“. *Der Tagesspiegel Online*. https://www.tagesspiegel.de/politik/eine-task-force-gegen-propaganda-6319330.html.

Schäfer, Claudia. 2023. „The Disinformation Landscape in Austria“. *EU DisinfoLab*. https://www.disinfo.eu/publications/disinformation-landscape-in-austria/.

Scherling, Laura S. 2025. *The Downfall of the Global Engagement Center and Disappearing Guardrails Against Disinformation*. https://doi.org/10.7916/38bc-7y91.

Schulze, Matthias. 2019. „Desinformation: Vom Kalten Krieg zum Informationszeitalter“. bpb.de, Mai 2. https://www.bpb.de/themen/medien-journalismus/digitale-desinformation/290487/desinformation-vom-kalten-krieg-zum-informationszeitalter/.

Serrano, Raguel Miguel. 2023. „The Disinformation Landscape in Germany“. *EU DisinfoLab*. https://www.disinfo.eu/publications/disinformation-landscape-in-germany/.

SGDSN. 2022. *National strategic review*. Secrétariat général de la Défense et de la Sécurité nationale. https://www.sgdsn.gouv.fr/files/files/rns-uk-20221202.pdf.

Shin, Jieun, und Kjerstin Thorson. 2017. „Partisan selective sharing: The biased diffusion of fact-checking messages on social media“. *Journal of communication* 67 (2): 233–55.

Standard. 2025. „Nationaler Sicherheitsberater Vorhofer: ‚Im hybriden Bereich sind wir schon im Krieg‘“. DER STANDARD, Mai 21. https://www.derstandard.at/story/3000000270699/nationaler-sicherheitsberater-vorhofer-im-hybriden-bereich-sind-wir-schon-im-krieg.

Sulzbacher, Markus. 2025. „Deutscher Verfassungsschutz überwacht Auf 1“. DER STANDARD, September 26. https://www.derstandard.at/story/3000000288102/deutscher-verfassungsschutz-ueberwacht-auf-1.

Tassinari, Fabrizio. 2016. *The Renationalisation of European Politics*. November 23. https://policycommons.net/artifacts/1330976/the-renationalisation-of-european-politics/1934293/.

Trpkovic, Mina. 2025. „Germany’s Fragmented Approach to Disinformation in 2025 Elections“. *PRIF BLOG*, Februar 3. https://blog.prif.org/2025/02/03/germanys-fragmented-approach-to-disinformation-in-2025-elections/.

UN. Human Rights Committee, Hrsg. 2004. *General comment no. 31 (80), The nature of the general legal obligation imposed on States Parties to the Covenant: International Covenant on Civil and Political Rights: adopted on 29 March 2004 (2187th meeting)*. UN. https://digitallibrary.un.org/record/533996.

Vargo, Chris J, Lei Guo, und Michelle A Amazeen. 2018. „The Agenda-Setting Power of Fake News: A Big Data Analysis of the Online Media Landscape from 2014 to 2016“. *New Media & Society* 20 (5): 2028–49. https://doi.org/10.1177/1461444817712086.

Veiga, Madalena de Almeida. 2025. *8 Combating Foreign Information Manipulation and Interference through EU-Restrictive Measures*. Brill. https://doi.org/10.1163/9789004700635_009.

VIGINUM. 2024a. *Foreign information manipulation and interference (FIMI) threat awareness - Guide for media and fact-checkers during the olympic and paralympic games*. Paris. https://www.sgdsn.gouv.fr/files/files/Publications/Guide_sensi_journalistes_english_vf.pdf.

VIGINUM. 2024b. *Portal Kombat - A structured and coordinated pro-russian propaganda network*. Technical Report. Paris. https://www.sgdsn.gouv.fr/files/files/20240212_NP_SGDSN_VIGINUM_PORTAL-KOMBAT-NETWORK_ENG_VF.pdf.

Wardle, Claire, und Hossein Derakhshan. 2017. *Information Disorder: Toward an interdisciplinary framework for research and policymaking*. Council of Europe.

Wheatley, Steven. 2020. „Foreign Interference in Elections under the Non-Intervention Principle: We Need to Talk About" Coercion"“. *Duke J. Comp. & Int'l L.* 31: 161.

Windwehr, Svea. 2025. „Trump vs. Europa: Welche Rolle der Digital Services Act spielt“. Heinrich Böll-Stiftung. https://www.boell.de/de/2025/02/05/trump-vs-europa-welche-rolle-der-digital-services-act-spielt.

Zeitlin, Jonathan. 2005. „Conclusion: The open method of coordination in action: Theoretical promise, empirical realities, reform strategy“. *The Open Method of Co-ordination in Action: The European Employment and Social Inclusion Strategies*, 447–503.

Zhang, Linda. 2020. „How to counter China's disinformation campaign in Taiwan“. *Military Review*, 21–32.