AUSTRIAN INSTITUTE FOR EUROPEAN AND SECURITY POLICY

Bundesministerium Landesverteidigung

Nr. 2022/1

Desinformation und Cyberangriffe

Europäische Antworten auf zunehmende hybride Bedrohungen

von Michael Zinkanell

Juni 2022

AIES STUDY

Executive Summary

Im Zeitraum der vorliegenden Analyse, Mitte 2021 bis Mitte 2022, lässt sich aus den sicherheitspolitischen Entwicklungen im Zusammenhang mit Cyberbedrohungen und Desinformationskampagnen auf die Europäische Union (EU) und ihre Mitgliedsstaaten eine Intensivierung der komplexen hybriden Bedrohungslage erkennen. Diese Zunahme der Aggression auf unkonventioneller Ebene und die damit verbundene Verschlechterung der allgemeinen Sicherheitslage innerhalb der EU lässt sich in erster Linie auf den russischen Angriffskrieg auf die Ukraine zurückführen. Bereits in den Monaten vor Beginn der russischen Invasion der Ukraine am 24. Februar 2022 kam es zu einem Anstieg von Desinformationskampagnen, die direkt den russischen Staatsmedien zugeordnet werden können. Darüber hinaus verzeichneten Expert:innen unmittelbar vor und in den Tagen nach Beginn des Angriffskriegs eine starke Zunahme von Cyberangriffen und Ransomware-Attacken auf die Ukraine selbst sowie eine Verschärfung von digitalen Angriffen auf EU-Mitgliedsstaaten während dem weiteren Kriegsverlauf.

Aus der Analyse dieser Angriffe und ihrer Muster geht hervor, dass Russland im Zuge der Invasion der Ukraine seine Angriffstaktik aus der Luft und auf dem Landweg auf hybride Mittel abstimmt. Somit kommt es zu einer systematischen Synchronisation von konventionellen und unkonventionellen Kriegsmitteln, welche den digitalen Raum zum Kriegsschauplatz macht. Damit geht die weitere Zuspitzung des sicherheitspolitischen Gefahrenpotentials des digitalen Informationsraums einher, ein Trend, der sich bereits seit den letzten Jahren sukzessive in Richtung einer zunehmenden Eskalation entwickelt. Vor diesem Hintergrund sind sich europäische Sicherheitsexpert:innen einig, dass gezielte Desinformationskampagnen und Cyberangriffe als Waffen des 21. Jahrhunderts betrachtet werden müssen, wie es sich unter anderem aus den Diskussionsergebnissen des Paris Cyber Summit 2022 ableiten lässt.

Als Reaktion auf die zunehmende hybride Unsicherheit sowie zur Stärkung der europäischen Resilienz, Sicherheit und Verteidigungsfähigkeit kam es in den letzten Monaten zu wesentlichen Weiterentwicklungen in Form von Strategien, Instrumenten und Gegenmaßnahmen auf EU-Ebene. Die folgenden Kapitel gehen strukturiert auf diese Entwicklungen im Cyberbereich sowie in der Bekämpfung von Desinformation ein. Abschließend bietet das Impulspapier einen Ausblick und skizziert Handlungsempfehlungen für österreichische Bedarfsträger:innen.

Inhaltsverzeichnis

Executive Summary 1
Inhaltsverzeichnis 2
1. Europäische Initiativen zum Ausbau von Cybersicherheit 2
1.1 Einrichtung eines Europäischen Kompetenzzentrums für Cybersicherheit 2
1.2 Prüfung des Potenzials einer gemeinsamen Cyber-Einheit 3
1.3 Die Um- und Einsetzung des Strategischen Kompasses im Kampf gegen Hybride Bedrohungen 3
1.4 Vorläufige Einigung über die NIS-2-Richtlinie 5
1.5 Verlängerung der Sanktionsregelung 6
1.6 EU Cyber Posture: Stärkung der Cybersicherheit und Verhinderung von Cyberangriffen 6
2. Europäische Maßnahmen zur Bekämpfung von Desinformationskampagnen 6
2.1 Europäische Vorschriften für politische Werbung, Wahlrecht und Parteienfinanzierung 6
2.2 Europäischer Rechtsakt zur Medienfreiheit 7
2.3 Europäische Sanktionspakete gegen Russland 7
2.4 Gestärkter Verhaltenskodex zur Bekämpfung von Desinformation 7
3. Conclusio 8

1. Europäische Initiativen zum Ausbau von Cybersicherheit

1.1 Einrichtung eines Europäischen Kompetenzzentrums für Cybersicherheit

Ende April 2021 gab der Europäische Rat grünes Licht zur Einrichtung des Europäischen Kompetenzzentrums für Cybersicherheit[1], welches in Bukarest errichtet werden soll. Die Verhandlungen dafür haben bereits 2020 während der Deutschen Ratspräsidentschaft ihren Anfang genommen. Mit dem neuen Kompetenzzentrum sollen Investitionen in Forschung, Technologie und industrielle Entwicklung im Bereich der Cybersicherheit zusammengeführt werden, um die Internetsicherheit zu erhöhen. Durch die Bündelung und verbesserte Koordinierung der Kompetenzen und Ressourcen im Cyberbereich auf europäischer Ebene ist eine Verbesserung der Forschung und Optimierung der digitalen Sicherheit möglich, welche auch wirtschaftliche Vorteile hinsichtlich der Aufwertung des europäischen Technologiestandortes und der Wettbewerbsfähigkeit mit sich bringen.

Darüber hinaus verfolgt das Cybersicherheit-Kompetenzzentrum den Ausbau der Cyberabwehrfähigkeit, die Unterstützung von Klein- und Mittelunternehmen im Bereich Cybersicherheit sowie die Stärkung der digitalen Souveränität Europas als übergeordnetes Ziel. Um auch auf der Ebene der Mitgliedsstaaten eine effizientere Zusammenarbeit sicherzustellen, wird das Europäische Kompetenzzentrum mit einem Netzwerk nationaler Zentren verflochten. Den österreichischen Netzwerkpartner stellt das „Nationale Koordinierungszentrum Cybersicherheit Österreichs“ dar, welches durch eine Kooperation zwischen dem Bundeskanzleramt und der Forschungsförderungsgesellschaft ins Leben gerufen wurde.[2]

1.2 Prüfung des Potenzials einer gemeinsamen Cyber-Einheit

Auf Empfehlung der Europäischen Kommission vom Juni 2021 beschloss der Europäische Rat im Oktober 2021 einen Impuls zu setzen, um den EU-Rahmen für das Krisenmanagement im Bereich der Cybersicherheit zu erweitern und dabei das Potenzial für eine gemeinsame Cyber-Einheit zu überprüfen. Um mögliche Lücken und fehlende Prozesse beim Interformationsaustausch innerhalb sowie zwischen europäischen Cybersicherheit-Gemeinschaften zu beheben sowie zur Konsolidierung bereits bestehender Netzwerke beizutragen, sollen Ziele und Potenziale einer gemeinsamen Cyber-Einheit[3] geprüft werden. Dieser gesamteuropäische Ansatz ist zielführend in der umfassenden Bekämpfung von Cybergefahren, welche die Schwachstellen im System sukzessive ausnutzen und keine nationalstaatlichen Grenzen kennen. Demnach wird erkannt, dass eine europäische Cybersicherheit nicht alleinig von den nationalen Fähigkeiten der Mitgliedsstaaten gedeckt werden kann und dass gesamtheitliche Kompetenzen und Strukturen notwendig sind.

Durch jene Initiative reagieren die europäischen Institutionen auf die steigende Anzahl an schwerwiegenden Cyberangriffen die nicht nur Einzelpersonen und Unternehmen treffen und wirtschaftlich schädigen, sondern auch nationale öffentliche Dienste einschränken und die demokratischen Fundamente der EU gefährden. In der Theorie würde eine gemeinsame EU-Cyber-Einheit eine Plattform für den Austausch von Ressourcen und Kenntnissen bieten und hinsichtlich präventiver und abschreckender Maßnahmen im Kampf gegen Cyberbedrohungen einen wesentlichen Beitrag leisten. Die konkreten Details über die praktische Ausgestaltung dieses Vorhabens stehen noch nicht fest. Um jedoch vom cyberspezifischen Wissensaustausch zu profitieren, besser gegen Cyberangriffe auf Politik bzw. Wirtschaft gewappnet zu sein und in einer gesamteuropäischen Cyberabwehr fest verankert zu sein, sollte sich Österreich proaktiv beteiligen.

1.3 Die Um- und Einsetzung des Strategischen Kompasses im Kampf gegen Hybride Bedrohungen

Im März 2022 wurde der viel diskutierte und lang angekündigte Strategische Kompass der EU vom Europäischen Rat veröffentlicht (gesamter Titel. „*Ein Strategischer Kompass für Sicherheit und Verteidigung – Für eine Europäische Union, die ihre Bürgerinnen und Bürger, Werte und Interessen schützt und zu Weltfrieden und internationaler Sicherheit beiträgt*“). Unter Hervorhebung der aktuellen und akuten geopolitischen Veränderungen, vernetzten Sicherheitsbedrohungen und strategischen Herausforderungen hat der Strategische Kompass den Anspruch richtungsweisend die Zukunft der europäischen Sicherheits- und Verteidigungspolitik zu gestalten[4]. Dabei verfolgt der Strategische Kompass vier konkrete Ziele:

1. eine gemeinsame Bewertung unseres strategischen Umfelds, der Bedrohungen und Herausforderungen, mit denen wir konfrontiert sind, und ihrer Auswirkungen auf die EU zu umfassen;
2. für mehr Kohärenz und ein gemeinsames Zielbewusstsein bei bereits laufenden Maßnahmen im Bereich Sicherheit und Verteidigung zu sorgen;
3. neue Wege und Mittel aufzuzeigen, um unsere kollektive Fähigkeit zur Verteidigung unserer Bürgerinnen und Bürger und unserer Union zu verbessern;
4. klare Zielvorgaben und Etappenziele zur Messung der Fortschritte zu enthalten.[5]

Hinsichtlich der Gefahrenlage durch hybride Bedrohungen wird gleich zu Beginn des Dokuments auf den Anstieg der Häufigkeit und der Intensität von unkonventionellen Angriffen aufmerksam gemacht. Darüber hinaus geht der Strategische Kompass sehr genau auf die Einzelheiten und den Umfang von hybriden Mitteln ein und findet klare Worte zur Definition der Bedrohungslage sowie zu den Ursprungsländern der hybriden Aggressionen. Auf diese deutliche, bestimmte und umfangreiche Art und Weise hat die EU davor noch nie die Taktiken und Akteure von hybriden Bedrohungen in einem Dokument erwähnt. Hier einige nennenswerten Textpassagen des Strategischen Kompasses hinsichtlich hybrider

Bedrohungen, Cyberangriffen und Desinformationskampagnen, welche auch die aktuellen Entwicklungen in der Ukraine widerspiegeln:

Die bewaffnete Aggression gegen die Ukraine zeigt die Bereitschaft, ungeachtet von rechtlichen oder humanitären Erwägungen ein Höchstmaß an militärischer Gewalt anzuwenden, ***verbunden mit hybriden Taktiken, Cyberangriffen, ausländischer Informationsmanipulation und Einmischung, wirtschaftlichem Druck und Druck auf den Energiesektor sowie aggressiver nuklearer Rhetorik****. Dieses aggressive und revisionistische Handeln, für das die russische Regierung zusammen mit ihrem Helfer Belarus in vollem Umfang verantwortlich ist, stellt eine ernste und unmittelbare Bedrohung für die europäische Sicherheitsordnung und die Sicherheit der europäischen Bürgerinnen und Bürger dar.*[6]

China tendiert zu Beschränkungen des Zugangs zu seinem Markt und versucht, die eigenen Standards weltweit zu fördern. Es verfolgt seine Politik durch eine zunehmende Präsenz auf See und im Weltraum sowie durch den Einsatz von ***Cyber-Tools und hybriden Taktiken****.*[7]

Staatliche und nichtstaatliche Akteure setzen hybride Strategien, Cyberangriffe, Desinformationskampagnen, direkte Einflussnahme auf unsere Wahlen und politischen Prozesse, wirtschaftlichen Druck sowie die Instrumentalisierung irregulärer Migrationsströme ein. Der zunehmende Missbrauch von Rechtsvorschriften zu politischen, wirtschaftlichen und militärischen Zwecken ist ebenfalls ein wachsendes Problem. Unsere Wettbewerber schrecken nicht davor zurück, neue und disruptive Technologien einzusetzen, um strategische Vorteile zu erzielen und die Wirksamkeit ihrer hybriden Kampagnen zu erhöhen. Einige haben die Unsicherheiten, die durch die COVID-19-Pandemie entstanden sind, genutzt, um schädliche und falsche Narrative zu verbreiten.[8]

In diesen Zeiten der zunehmenden Abhängigkeit von digitalen Technologien ist der ***Cyberraum zum Schauplatz eines strategischen Wettbewerbs geworden****. Wir sind zunehmend mit ausgefeilteren Cyberangriffen konfrontiert. Es gilt unbedingt, einen offenen, freien, stabilen und sicheren Cyberraum aufrechtzuerhalten.*[9]

Ganz im Sinne der Zielsetzung des Strategischen Kompasses, zählt das Dokument nicht nur sicherheits- und verteidigungspolitisch relevante Herausforderung für die EU und ihre Mitgliedsstaaten auf, sondern legt konkrete Schritte und Handlungsoptionen dar, die sich entlang Maßnahmen in vier Arbeitsbereichen orientieren (*Handeln*, *Sichern*, *Investieren*, und *mit Partnern zusammenarbeiten*). Auch diese Schwerpunktsetzung, die einleitende problemzentrierte Darlegung hybrider Bedrohungen mit greifbaren und lösungsorientierten Ansätzen zu ergänzen, erweist sich als innovatives Charakteristikum des Strategischen Kompasses. Somit handelt es sich beim Strategischen Kompass um die elegante Kombination aus einem zukunftsweisenden Strategiepapier sowie einem praktischen Maßnahmenkatalog.

Hinsichtlich der Bekämpfung verschiedener hybrider Bedrohungen fordert der Strategische Kompass folgende wesentliche Umsetzungsschritte in allen vier Bereichen:

<u>Handeln:</u>

- Durchführung von gemeinsamen EU-Cyberübungen als Ergänzung der regelmäßigen Übungen zur weiteren Festigung der gegenseitigen Unterstützung im Falle eines bewaffneten Angriffs auf ein EU-Mitglied.
- Erhöhung der Cyberresilienz und Nutzung von künstlicher Intelligenz zur Verbesserung der militärischen Mobilität.

<u>Sichern:</u>

- Die Schaffung eines hybriden EU-Instrumentariums, in welchem diverse Instrumente und Ansätze zusammengefasst werden sollen, damit die Erkennung von und Reaktion auf hybride Bedrohungen verbessert werden kann. Zusätzlich soll das Analyseverfahren von hybriden Bedrohungen vereinheitlicht werden, um eine verbesserte Vorausschau und Lageeinschätzung zu ermöglichen.
- Die Weiterentwicklung der EU-Cyberabwehrpolitik zur effektiveren Vorbereitung auf und Abwehr von Cyberangriffen, sowie die Stärkung des EU-Instruments für Cyberdiplomatie einschließlich der Präventions- und Sanktionsmaßnahmen

und der Ausbau der europäischen Kapazitäten im Bereich Cyberaufklärung.

- Entwicklung eines speziellen Instrumentariums zur Verhinderung von ausländischen Informationsmanipulationen und Einflussnahmen. Darunter fallen verbesserte Möglichkeiten der Analyse und Abwehr von Bedrohungen im Informationsraum, der Ausbau der Strategischen Kommunikation der EU, sowie der Ausbau von Maßnahmen zur Bekämpfung von Desinformation.

Investieren:

- Ausbau einer raschen Cyberabwehr innerhalb bestehender Strukturen der Ständigen Strukturieren Zusammenarbeit sowie des Europäischen Verteidigungsfonds und Reduzierung von Defiziten im Bereich der Cyberabwehrfähigkeiten.
- Weiterentwicklung und Investition in neue Technologien im Bereich der Quantentechnologie, künstlichen Intelligenz und Big Data, um europäische Cyberabwehr und Informationssicherheit zu stärken.

Mit Partnern zusammenarbeiten:

- Ausbau und Stärkung der transatlantischen Partnerschaft in der Abwehr von hybriden Bedrohungen wie unter anderem externe Informationsmanipulationen, Desinformationskampagnen und subversive Einmischung. In diesem Zusammenhang sollen Synergien in der Zusammenarbeit mit der NATO gestärkt werden.
- Ausweitung der strategischen Dialoge und der Strategischen Kommunikation in der Zusammenarbeit mit den Ländern der Östlichen Partnerschaft, um hybride Gefahren zu mildern und die Cyber- und Informationssicherheit auszubauen.
- Engere Zusammenarbeit mit den Ländern der südlichen Nachbarschaft, des Westbalkans sowie der europäischen Partner in Afrika zur Stärkung der Resilienz gegenüber hybriden Bedrohungen durch den Aufbau von Kapazitäten, Schulungen und Mittelaufstockung.

Aus den hier skizierten Inhalten zur Verbesserung der Cyberabwehr, Informationssicherheit bzw. Resilienz gegenüber hybriden Angriffen allgemein geht hervor, dass Komplexität der Problematik erkannt wurde und innovative Lösungsansätze erarbeitet wurden, um auf die zunehmende Gefahrenlage einzugehen. Stärker als in der Vergangenheit präsentiert die EU hierbei proaktive und präventive Maßnahmen und geht nicht primär auf reaktionäre Aspekte ein. Darüber hinaus versteht sich der Strategische Kompass keinesfalls als ein starres Dokument, denn es wird nicht nur die Vorlegung eines Jahresfortschrittsberichts gefordert, sondern auch die etwaige Überarbeitung des Kompasses im Jahr 2025. Somit geht man direkt und selbstbewusst auf die sich verändernde Bedrohungen ein, welche sich insbesondere im hybriden Bereich manifestieren. Eine stände Weiterentwicklung der Strategien und Maßnahmen ist daher unerlässlich, womit der Strategische Kompass durch seine notwendige Flexibilität und Anpassungsfähigkeit zum perfekten Vehikel auszeichnet. Nichtsdestotrotz muss abgewartet werden, wie sich die unmittelbare Umsetzung der Ziele praktisch entwickelt, mit welcher Begeisterung die Mitgliedsstaaten an der gesamteuropäischen Weiterentwicklung von Kompetenzen wirklich beteiligt sein wollen und ob die ambitionierten Ziele des Strategischen Kompasses in der Tat die gewünschte Wirkung erzielen.

1.4 Vorläufige Einigung über die NIS-2-Richtlinie

Im Mai 2022 einigten sich der Europäische Rat und das Europäische Parlament auf Maßnahmen zur Verbesserung der Reaktionsmöglichkeiten sowie zum Aufbau von Kapazitäten, um gegen Cyberangriffe besser gewappnet zu sein. Damit geht die Schaffung einer neuen Richtlinie zur Netz- und Informationssicherheit[10] (NIS 2) einher, welche die bereits seit 2016 bestehende NIS 1 Richtlinie ersetzen soll. Damit wird die NIS 2 Richtlinie zur Basis für die Maßnahmen des Cybersicherheitsrisikomanagements und der Meldepflicht für alle nationale Sektoren wie u.a. Verkehr, Gesundheit, Energie und digitale Infrastruktur.

Durch die Neugestaltung der Richtlinie sollen Differenzen bei den Anforderungen an die nationale Cybersicherheit sowie bei der Einführung von unterschiedlichen Cybersicherheitsmaßnahmen zwischen EU-Mitgliedsstaaten behoben werden. Außerdem sollen durch Mindestvorschriften für den Rechtsrahmen und die jeweiligen Mechanismen

eine effektive behördenübergreifende Zusammenarbeit ermöglicht werden. Um die Auswirkung von zunehmenden Cyberangriffen auf öffentliche Verwaltungseinrichtungen zu mindern, soll die NIS 2 Richtlinie darüber hinaus auch für Einrichtungen der öffentlichen Verwaltung auf staatlicher und regionaler Ebene gelten. Ob die lokale Verwaltungsebene ebenfalls in die Richtlinie aufgenommen werden soll, obliegt den Mitgliedsstaaten selbst. Die EU-Mitgliedsstaaten haben nach dem Inkrafttreten der NIS 2 Richtlinie 21 Monate Zeit, um die Vorschriften in nationales Recht einzubetten.

1.5 Verlängerung der Sanktionsregelung

Der Europäische Rat beschloss Mitte Mai 2022 die Rahmenbedingungen der Sanktionsregelung[11] gegen Personen bzw. Organisationen, die an Cyberangriffen gegen die EU oder ihre Mitgliedsstaaten beteiligt sind, um drei Jahre bis 2025 zu verlängern. Ziel der restriktiven Maßnahmen ist Cyberbedrohungen einzuschränken bzw. durch Abschreckung Cyberangriffen vorzubeugen sowie Entschlossenheit in der Zuordnung und rechtlichen Ahndung von digitalen Angriffen zu projizieren. Derzeit sind acht Personen und vier Organisation von den Sanktionen betroffen, welche Reiseverbote sowie das Einfrieren von Vermögen umfassen. Die Sanktionsregelung stellt ein effektives Mittel innerhalb der Handlungsfähigkeit der EU dar, welches gezielt gegen ausführende sowie finanziell unterstützende Hintermänner von Cyberangriffen vorgeht. Um noch umfassender auf die Vielzahl an verschiedenen hybriden Bedrohungen vorzugehen, wäre es zielführend die Sanktionsmechanismen auch auf andere unkonventionelle Angriffsformen anzuwenden.

1.6 EU Cyber Posture: Stärkung der Cybersicherheit und Verhinderung von Cyberangriffen

Als erste direkt Umsetzung der cybersicherheitsrelevanten Vorhaben des Strategischen Kompasses, beschloss der Europäische Rat Ende Mai 2022 eine europäische „Cyber Posture“[12] (Cyber-Haltung) zu entwickeln. Das Ziel der Initiative ist europäische Entschlossenheit zu demonstrieren im Zuge der langfristigen und unmittelbaren Reaktionen auf Bedrohungen im Cyberraum.

Konkret umfassen die vorgeschlagenen Cybersicherheitsinitiativen fünf Schwerpunkte: die Stärkung der Resilienz und Kapazitäten, Verbesserun des umfassenden Krisenmanagements, Förderung der EU-Vision für einen freien und sicheren Cyberraum, Ausbau der Kooperationsformate mit Partnerländern und internationalen Organisationen sowie die Verhinderung und Verteidigung gegen Cyberangriffen. Um die konkrete Umsetzung der Initiative voranzutreiben, ist die Agentur der Europäischen Union für Cybersicherheit (ENISA) zudem mit der Ausarbeitung von Vorschlägen und Empfehlungen beauftragt worden.

2. Europäische Maßnahmen zur Bekämpfung von Desinformationskampagnen

2.1 Europäische Vorschriften für politische Werbung, Wahlrecht und Parteienfinanzierung

Um nicht nur gegen externe Desinformationskampagnen und äußere demokratiegefährdende Einflussnahme gewappnet zu sein, legte die Europäische Kommission im November 2021 einen neuen Vorschlag über die Verbesserung der Transparenz und Ausrichtung von politischer Werbung vor. [13] Als Teil neuer Maßnahmen zum Schutz der Integrität von demokratischen Wahlen in Europa sowie der Förderung von politischer Partizipation, soll die Kennzeichnung von politischer Werbung noch deutlicher vorgeschrieben werden unter Angabe der Kosten für die jeweilige Werbekampagne. Ziel ist es, der europäischen Bevölkerung eine leichtere Erkennung von bezahlten politischen Inhalten und Wahlwerbung auf allen Medien zu ermöglichen, um demokratiepolitische Entscheidungen unvoreingenommener und ohne manipulative Einflüsse vornehmen zu können.

Darüber hinaus werden strengere Auflagen für politisches Targeting empfohlen, um Techniken des emotionalen Verstärkens von politischen Inhalten, u.a. durch die Verwendung von personenbezogenen Daten wie ethnischer Herkunft oder religiöser Zuordnung, zu unterbinden. Als weitere Schritte sollen

die Vorschläge nun im Europäischen Rat und im Europäischen Parlament diskutiert werden. Zur Sicherstellung des höchsten demokratischen Standards bei den nächsten Wahlen zum EU-Parlament 2024, sollen aus den vorliegenden Vorschlägen bis Anfang 2023 neue Vorschriften abgeleitet und in Folge umgesetzt werden. Eine verstärkte Sensibilisierung der europäischen Bevölkerung für subtile Methoden der politischen Manipulation und Einflussnahme würde auch zur Bewusstseinsbildung über die Gefahren von Desinformationskampagnen positiv beitragen.

2.2 Europäischer Rechtsakt zur Medienfreiheit

Zur Sicherstellung der Unabhängigkeit der europäischen Medien sowie zur Förderung des Pluralismus hat die Europäische Kommission im Jänner 2022 eine öffentliche Konsultation zum geplanten europäischen Rechtsakt zur Medienfreiheit bekannt gemacht.[14] Zwischen Jänner und März 2022 konnten Behörden, Medienakteure und Privatpersonen sich über einen Fragebogen direkt an dem Prozess beteiligen sowie ihre Meinung zu den Vorschlägen zur Förderung der Medienfreiheit einbringen. Darunter fallen Initiativen wie die Bekämpfung von Desinformation, Stärkung der demokratischen Teilhabe sowie die Sicherstellung der Freiheit der Medien, welche auf den Aktionsplan für Demokratie zurückzuführen sind. Die Vorschläge zum Rechtsakt zur Medienfreiheit sollen der Europäischen Kommission im dritten Quartal 2022 präsentiert werden, woraus sich die nächsten Schritte ableiten werden.

2.3 Europäische Sanktionspakete gegen Russland

Als Reaktion des russischen Angriffskriegs auf die Ukraine, verabschiedete die EU bislang insgesamt sechs umfassende Sanktionspakete.[15] Die vielseitigen und in diesem Ausmaß noch nie dagewesenen europäischen Sanktionen gegenüber Russland werden als eines der effektivsten und unmittelbarsten Mittel der EU angesehen, um die russische Wirtschafts- und Exportleistung zu schwächen, den russischen Einfluss zu vermindern und Einzelpersonen für die Unterstützung des illegitimen Angriffskriegs sowie die Durchführung der russischen Gräueltaten zu ahnden. Neben weitreichenden zusätzlichen restriktiven Maßnahmen erließ die EU im Zuge der Sanktionen, dass die Sendetätigkeit von fünf russischen Staatsmedien innerhalb der EU auszusetzen, um die Verbreitung von Desinformation und russischer Propaganda zu unterbinden.

Die Sendetätigkeit der beiden Medien „Sputnik“ und „Russia Today“, welche unter ständiger direkter bzw. indirekter Kontrolle des Kremls stehen, wurde bereits im Zuge des dritten Sanktionspakets Anfang März eingestellt,[16,17] gefolgt von der Erweiterung auf drei zusätzliche Staatsmedien „Rossiya RTR / RTR Planeta“, „Rossiya 24/Russland 24“ sowie „TV Centre International“ im Zuge des sechsten Sanktionspakets von Anfang Juni 2022. Damit wird erreicht, dass die zentralsten kremlfreundlichen Sender ihre Desinformations- und Informationsmanipulationsmaßnahmen gegen die EU und ihre Mitgliedstaaten nicht mehr fortsetzen können. Dies betrifft sowohl die Verbreitung von Inhalten über Kabel und Satellit als auch das Internet sowie digitale Applikationen. Die Europäische Union beugt mit dieser Maßnahme einer zunehmenden Instrumentalisierung dieser Medien als Mittel zur Manipulation und Destabilisierung der europäischen Bevölkerung vor. Da es sich bei den sanktionierten Medien nicht um eine unabhängige Berichterstattung handelt, sondern um die Erstellung und Verbreitung von gezielten Falschinformationen zu politischen Propagandazwecken, schränken die Sanktionen nicht die europäische Medien- oder Meinungsfreiheit ein.

2.4 Gestärkter Verhaltenskodex zur Bekämpfung von Desinformation

Aufbauend auf die wegweisende erste Version des Kodexes von 2018, wurde Mitte Juni 2022 der neue Verhaltenskodex zur Bekämpfung von Desinformation unterzeichnet und veröffentlicht. Unter den 34 Unterzeichnern befinden sich digitale Plattformen und Unternehmen aus der Technologiebranche (u.a. Meta, Google, Twitter, TikTok und Microsoft) sowie zivilgesellschaftliche Organisationen, welche sich in Eigenverantwortung zur Umsetzung der neuen Leitlinien vom Mai 2021 bereit erklärt haben. Die Lehren aus der COVID-19 Krise sowie aus den russischen Propagandameldungen und Desinformationen im Zuge des Angriffskriegs auf die Ukraine fließen vor diesem Hintergrund in den neuen Verhaltenskodex mit ein.

Der neue Verhaltenskodex zur Bekämpfung von Desinformation enthält unter anderem folgende Verpflichtungen[18]:

- Keine Werbeeinnahmen für Akteure, die Desinformation verbreiten, damit geringere monetäre Anreize für die Erstellung und Verbreitung von Desinformation geschaffen werden;
- Analyse der Methoden und Verhaltensweisen von Desinformationsakteuren sowie die Erfassung von neuen technologischen Manipulationsmöglichkeiten (Bots bzw. Deepfakes);
- Möglichkeit der breiteren Beteiligung am Verhaltenskodex durch die Inklusion einer Vielzahl von diversen Akteuren, welche für die Bekämpfung von Desinformation essenziell sind;
- Schaffung von Möglichkeiten und Instrumenten für Nutzer:innen von digitalen Plattformen und Medien zur leichtere Erkennung von Desinformation;
- Mehr Unterstützung für die Erforschung von Desinformation, erleichterter Datenzugang, sowie Ausweitung der Faktenprüfung auf alle EU-Länder und EU-Sprachen.

Nach der Unterzeichnung haben die Plattformen, Organisationen und Medienbetreiber sechs Monate Zeit, um die Maßnahmen einzuleiten und bis Anfang 2023 der Europäischen Kommission einen Umsetzungsbericht vorzulegen. Betreiber von digitalen Informationen vermehrt in die Bekämpfung von Desinformation zu integrieren bzw. in die Verantwortung zu nehmen, ist ein wesentlicher Schritt, um eine ganzheitliche Einschränkung von manipulativen Inhalten sicherzustellen.

3. Conclusio

Aus den jüngsten Entwicklungen hinsichtlich hybrider Bedrohungen auf die EU und ihre Mitgliedsstaaten, insbesondere durch Desinformationskampagnen und Cyberangriffe, entwickelt sich der Trend konstant weiter Richtung einer Intensivierung der Bedrohungslage sowie der Synchronisation von hybriden und konventionellen Angriffstaktiken.

Diese Tendenz wird seit den vergangenen Jahren von zwei Hauptfaktoren befeuert: die Implikationen der COVID-19 Pandemie sowie technologische Weiterentwicklungen, welche auch die ENISA in ihrem jüngsten Bedrohungsbild hervorhebt.[19] Insbesondere neue technologische und digitale Anwendungsbereiche, wie u.a. aus dem Feld der Künstlichen Intelligenz sowie der Einsatz von Deepfakes (welchem erst kürzlich auch der Wiener Bürgermeister zum Opfer gefallen ist), stellen ernstzunehmende Sicherheitsbedrohungen dar. Hierbei muss in jeden Fall mehr öffentliches und sicherheitspolitisches Bewusstsein aufgebaut werden, um der Ernsthaftigkeit der Bedrohungslage gerecht zu werden.

Darüber hinaus hat der russische Angriffskrieg auf die Ukraine nicht nur zu einer Eskalation der konventionellen Kriegsführung auf dem Land-, See-, und Luftweg geführt, sondern auch eine enorme Intensivierung der russischen hybriden Angriffe eingeleitet. Obwohl diese hybriden Kriegstaktiken medial und in der öffentlichen Wahrnehmung von den robusten physischen Angriffen überschattet werden, dürfen sie in der Analyse der gewaltvollen Entwicklungen sowie der Untersuchung der russischen strategischen und operativen Kriegsführung nicht vernachlässigt werden.

Aus der Beobachtung der russischen Angriffstaktik auf ukrainische Ziele ergibt sich eine zentrale Ableitung für die Europäische Union: Russland kombiniert konventionelle und hybride Angriffe auf systematische Art und Weise und inkludiert somit digitale Ziele (mit oder ohne physische Auswirkungen) in die Taktiken seiner Kriegsführung. Zusätzlich zu den digitalen Angriffen auf die Ukraine selbst, kam es seit Ende Februar 2022 zu massiven russischen hybriden Attacken auf andere Staaten und Institutionen.

Basierend auf einer kürzlich erschienenen Analyse von Microsoft, welche die ersten Erkenntnisse des russischen Cyberkriegs im Zuge des Angriffskriegs auf die Ukraine untersucht, kam es seit Februar weltweit zu 128 russischen digitalen Cyber- und Netzwerkangriffen in 42 Ländern – wobei sich dabei knapp die Hälfte der Angriffe gegen öffentliche Einrichtungen und Regierungsbehörden richteten – kombiniert mit einem drastischen Anstieg an russischen Desinformationskampagnen.[20] EU-Mitgliedsstaaten sind in erster Linie von diesen Angriffen betroffen. Zusätzlich dazu prognostiziert das European

Centre of Excellence for Countering Hybrid Threats, dass Russland zeitgleich zum Angriffskrieg in der Ukraine seinen Einfluss im Mittleren Osten und Nordafrika mittels hybrider Angriffe erweitert.[21] Somit wurde durch die russische Aggression seit Februar 2022 Europa zum Schauplatz eines konventionellen und hybriden Kriegs, bei gleichzeitiger weitreichender Destabilisierung der unmittelbaren europäischen Nachbarschaft im Osten und Süden sowie direkten digitalen Angriffen auf die EU und ihre Mitgliedsstaaten.

About the Author

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

[1] Europäischer Rat, 2021: „Kompetenzzentrum für Cybersicherheit in Bukarest: Rat gibt grünes Licht.“, 20. April 2021

[2] Österreichische Forschungsförderungsgesellschaft (FFG), 2022: „Nationales Koordinierungszentrum Cybersicherheit“

[3] Europäischer Rat, 2021: “Cybersicherheit: Rat nimmt Schlussfolgerungen zur Prüfung des Potenzials einer gemeinsamen Cyber-Einheit an.“, 19. Oktober 2021

[4] Europäischer Rat, 2022: “Ein Strategischer Kompass für Sicherheit und Verteidigung.“, (7371/22) am 21. März 2022

[5] Europäischer Rat, 2022: “Ein Strategischer Kompass für Sicherheit und Verteidigung.“, (7371/22) am 21. März 2022, S.2

[6] Ibid., S.7

[7] Ibid., S.8

[8] Ibid., S.11

[9] Ibid., S.12

[10] Europäischer Rat, 2022: „Stärkung der EU-weiten Cybersicherheit und Resilienz – vorläufige Einigung zwischen Rat und Europäischem Parlament.“, 13. Mai 2022

[11] Europäischer Rat, 2022: „Cyberangriffe: Rat verlängert Sanktionsregelung bis zum 18. Mai 2025“, 16. Mai 2022

[12] Europäischer Rat, 2022: „Council conclusions on the development of the European Union's cyber posture.”, Schlussfolgerung (9364/22) am 23 Mai 2022

[13] Europäische Kommission, 2021: “Demokratie in Europa: Kommission legt neue Vorschriften für politische Werbung, Wahlrecht und Parteienfinanzierung fest.”, 25 November 2021

[14] Europäische Kommission, 2022: “Europäischer Rechtsakt zur Medienfreiheit: Kommission leitet öffentliche Konsultation ein.”, 10 Januar 2022

[15] Europäische Kommission, 2022: “Russlands Krieg gegen die Ukraine: EU verabschiedet sechstes Sanktionspaket gegen Russland”, 3 Juni 2022

[16] Europäischer Rat, 2022: „Restriktive Maßnahmen der EU gegen Russland aufgrund der Krise in der Ukraine (seit 2014) – EU Sanktionen im Überblick“

[17] Europäische Kommission, 2022: “Ukraine Sanktionen gegen die vom Kreml unterstützte Medien Russia Today und Sputnik” 2 März 2022

[18] Europäische Kommission, 2022: „Der Verhaltenskodex für Desinformation von 2022“, 29. Juni 2022

[19] ENISA, 2021: „ENISA Threat Landscape 2021 – April 2020 to mid-July 2021“, October 2021

[20] Microsoft, 2022: „Defending Ukraine: Early Lessons from the Cyber War“, 22. Juni 2022

[21] The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), 2022: „Due to its war in Ukraine, Russia may increase its hybrid threat activities in the MENA region“, 16. März 2022

Dr. Langweg 3, 2410 Hainburg/Donau

Tel. +43 (1) 3583080

office@aies.at | www.aies.at

Layout Design: Julia Drössler