AUSTRIAN INSTITUTE FOR EUROPEAN AND SECURITY POLICY

Bundesministerium Landesverteidigung

Nr. 2021/5

Desinformation und Cyberangriffe

Auf die EU im Zuge der COVID-19 Krise

von Michael Zinkanell

Juni 2021

AIES STUDY

Executive Summary

Die folgende AIES Studie wurde im Auftrag des Bundesministeriums für Landesverteidigung (BMLV) verfasst. Aus den aktuellen sicherheitspolitischen Entwicklungen im Zusammenhang mit Desinformation und Cyberangriffen auf die Europäische Union im Zuge der COVID-19 Krise geht hervor, dass die hybride Bedrohungslage an Intensität und Komplexität innerhalb der letzten 12-18 Monate zugenommen hat.

Die EU und ihre Mitgliedsstaaten sind seit Anfang 2020 mit subversiven Desinformationskampagnen sowie einer massiven Anzahl an Cyberangriffen konfrontiert, welche die generelle Unsicherheit und die vielschichtigen Folgewirkungen der Pandemie direkt ausnutzen. Aus der Analyse der Bedrohungslage geht hervor, dass jene hybriden Angriffe direkt auf die Destabilisierung der Union abzielen und Aggressoren die Grenzen ihrer Einflussnahme immer weiter austesten. Die modernen technologischen Mittel der Digitalisierung und die damit einhergehenden Abhängigkeiten befeuern das Gefahrenausmaß zunehmend.

Im Vergleich zu den Vorjahren besteht heute auf EU-Ebene ein erhöhtes Bewusstsein sowie eine Effizienzsteigerung und Weiterentwicklung der Gegenmaßnahmen zur Erkennung und Bekämpfung von hybriden Bedrohungen. Trotzdem sind die europäischen Strategien in erster Linie als reaktionär einzustufen, was eine proaktivere europäische Haltung umso notwendiger macht. Denn für die Gegenwart und Zukunft gilt, dass die Eintrittswahrscheinlichkeit und das Schadausmaß von Desinformationskampagnen und Cyberangriffen auf die Europäische Union mit sehr hoch zu beurteilen ist.

Inhaltsverzeichnis

1. Einleitung

Seit dem 1. Quartal 2020 und somit im Zuge der COVID-19 Krise intensivierte sich die Bedrohungslage durch hybride Gefahren innerhalb der Europäischen Union (EU). Insbesondere Desinformationskampagnen und Cyberangriffe nahmen in zweierlei Hinsicht zu: Einerseits häufte sich Anzahl der Vorfälle während andererseits die Intensität der Angriffe zeitgleich zunahm. In der Analyse der europäischen Cyber-Bedrohungen stellte die European Union Agency for Cybersecurity (ENISA) fest, dass Cyberangriffe raffinierter und gezielter werden, im größeren Umfang stattfinden und Großteils unerkannt bleiben.[1]

Allein im Zeitraum von Jänner 2019 bis April 2020 wurden täglich 230.000 neue Malware-Infektion erfasst[2] und die Gefahrenbeurteilung (2021) von EUROPOL hebt zusätzlich die deutliche Steigerung von Ransomware-Angriffen hervor.[3] Auch im Kontext der österreichischen Unternehmenslandschaft zeichnen sich ähnliche Entwicklungen ab. Anhand einer 2021 durchgeführten Umfrage von über 400 Unternehmen in Österreich geht hervor, dass 2020 60% der befragten Unternehmen Cyberangriffen zum Opfer fielen und knapp 40% eine Zunahme von Angriffen im Cyberraum feststellten.[4] Dies stellt einen klaren Anstieg gegenüber dem Vorjahr dar. Außerdem wurden im Zusammenhang mit der Entwicklung und Verteilung von COVID-Impfstoffen kritische Informationen sowie Lieferketten und Kühlsysteme zu neuen Zielen von Cyberangriffen, die unter anderem darauf abzielen geistiges Eigentum und Wissen, um die Impfstoffherstellung zu stehlen.

Im Zuge von Desinformationskampagnen kam es ebenfalls zu einem Anstieg der gezielten Falschmeldungen, welche auf die Destabilisierung der Europäischen Union und ihrer Mitgliedsstaaten abzielen. Jene Kampagnen nutzten die allgemeine Unsicherheit der COVID-19 Krise systematisch aus und bedienten sich einer Vielzahl (an teils widersprüchlichen) Narrativen rund um das COVID-19 Virus. Hierzu fand der Hohe Vertreter und Vizepräsident der EU-Kommission Josep Borrell scharfe sowie warnende Worte: *„Desinformation in Zeiten der Coronavirus-Pandemie kann töten. Wir haben die Pflicht, unsere Bürgerinnen und Bürger zu schützen, indem wir sie auf falsche Informationen aufmerksam machen und die für solche Praktiken verantwortlichen Akteure aufdecken.“*[5]

Bereits im März 2020 einigten sich die europäischen Staats- und Regierungschefs und entschieden gegen die Verbreitung von Desinformation und ihre Folgewirkungen vorzugehen. Auf EU-Ebene hat die Europäische Kommission in enger Zusammenarbeit mit dem Europäischen Auswärtigen Dienst (EAD) die strategische Kommunikation intensiviert, um nicht nur innerhalb der EU, sondern auch in der europäischen Nachbarschaft gegen Desinformationskampagnen vorzugehen.[6] Dabei wurde die Analyseplattform EUvsDisinfo, ein Leuchtturmprojekt der East Stratcom Task Force des EAD, maßgeblich zur Aufdeckung und Untersuchung von COVID-19 Desinformation eingesetzt. Seit Anfang 2020 wurden hunderte Fälle von nachweislich falschen Informationen im Zusammenhang mit dem Virus registriert und

analysiert, um Methoden, Muster und Narrative besser zu erkennen.

Dieses Impulspapier beleuchtet die aktuellen Bedrohungen, die von Cyberangriffen und Desinformationskampagnen ausgehen und eine unmittelbare Gefährdung für die EU sowie ihre Mitgliedsstaaten darstellen. Im Folgekapitel werden zunächst Cyberbedrohungen und Desinformation in den Kontext der hybriden Kriegsführung gesetzt, um die dahinterliegenden Strategien der Machtausübung anzuschneiden. Anschließend werden die jüngsten Entwicklungen der Bedrohungslandschaft im Bereich der Cyber- und Informationssicherheit mit einem Fokus auf den Zeitraum der COVID-19 Pandemie (Anfang 2020 bis Mitte 2021) behandelt. In diesem Zusammenhang werden auch die politischen und strategischen Gegenmaßnahmen auf Ebene der EU-Institutionen diskutiert. Abschließend bietet das Fazit neben einem Ausblick auf zukünftige Trends auch konkrete Handlungsoptionen und Politikempfehlungen für Entscheidungsträger:innen.

2. Desinformationskampagnen und Cyberangriffe als hybride Bedrohungen

Als unkonventionelle Art der Kriegsführung finden hybride Bedrohungen unterhalb der Schwelle zur formellen Kriegsführung statt. Die Gewaltanwendung geschieht oft nicht direkt auf physische Art, sondern in Form subtiler und oftmals subversiver indirekter diplomatischer, militärischer, wirtschaftlicher oder technologischer Machtausübung. Dabei verschleiern stattliche Akteure die Spuren ihrer Angriffe, bedienen sich Stellvertretern (Proxies) und entgehen durch die unvollständige bzw. inkonsistente Zurechenbarkeit den Konsequenzen ihrer aggressiven Einflussnahme.

Das Bedrohungsbild der hybriden Angriffe erstreckt sich daher über das Spektrum von Cyberattacken, zur Einflussnahme auf demokratische Entscheidungsprozesse, die Manipulation sozialer Medien und massiven Desinformationskampagnen. Eine einheitliche (staatlich, wissenschaftlich) Begriffsbestimmung hybrider Bedrohungen besteht jedoch

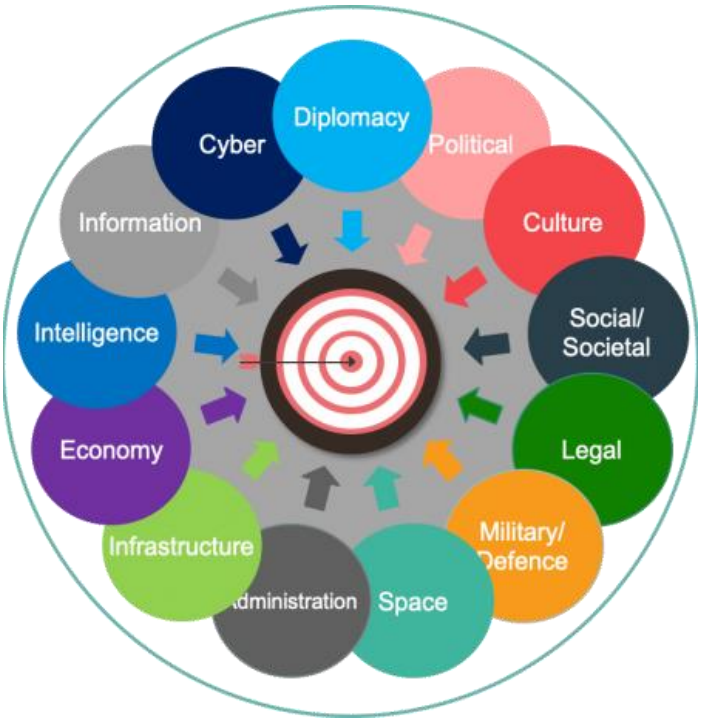

Abbildung 1 – Domänen der hybriden Bedrohung. Quelle: EU-HYBNET

nicht, was auch der fluiden sowie unkonventionellen Natur der Angriffe geschuldet ist. Fest steht, dass Akteure eine Vielzahl an hybriden Mitteln gezielt und aufeinander abgestimmt zum Einsatz bringen. Abbildung 1 veranschaulicht das umfangreiche Repertoire der hybriden Instrumente und illustriert die Vernetzung der einzelnen Aspekte, welche gebündelt übergeordnete Ziele verfolgen.[7]

Die expliziten Intentionen und Motivationen hinter hybriden Taktiken sind von Fall zu Fall und Angreifer zu Angreifer unterschiedlich, weisen aber gewisse Gemeinsamkeiten auf. Prinzipiell nutzen hybride Provokationen Schwachstellen im politischen, ökonomischen bzw. sozialen Systemen aus und beabsichtigen eine gesellschaftliche Destabilisierung. Dabei diskreditieren bzw. unterminieren Akteure wiederholt demokratische Regierungen durch das Schüren von Misstrauen und Polarisierung und schwächen somit die innere Kohärenz der EU. Einzelne Angriffe auf europäische Staaten können sich vor diesem Hintergrund spezifisch gegen die jeweiligen nationalen Regierungen richten. In einem größeren Zusammenhang zielen die koordinierten und langfristigen hybriden Taktiken jedoch auf die Aushöhlung der EU und ihrer Institutionen ab.

Es ist zudem erwähnenswert, dass hybride Bedrohungen keine Erfindung der modernen Kriegsführung sind. Als Mittel zur Täuschung und Verwirrung des Feindes sind hybride Mittel so alt wie das Wissen um die Strategien des Krieges selbst und stellen somit kein neuartiges Phänomen an sich dar. Bereits Sun Tzu beschrieb vor 2.500 Jahren in seinem zeitlosen Werk „Die Kunst des Krieges" Strategien und Taktiken um den Feind durch Falschinformationen zu schwächen. Jedoch spielen die Fortschritte der Digitalisierung eine maßgebliche Rolle, welche die Auswirkungen und Reichweite von hybriden Bedrohungen – insbesondere von Cyberangriffen und Desinformationskampagnen – enorm potenziert.

Die heutigen technologischen Instrumente ermöglichen einerseits Informationen und Daten mit simplen Mitteln zu manipulieren und missbrauchen. Dieselben Codes, welche man zur Erstellung von digitalen Anwendungen verwendet, werden somit als Mittel zum Zweck der Spionage, Infiltrierung bzw. Zerstörung von Systemen eingesetzt.[8] Im Falle von Desinformation können irreführende Inhalte mittels Sozialen Medien sehr einfach zirkuliert und mittels Algorithmen zielgruppengetreu platziert werden.

Andererseits basieren die heutigen (europäischen und großteils auch weltweiten) politischen, ökonomischen und sozialen Systeme auf der Abhängigkeit von digitalen Dienstleistungen, Produkten und Kommunikationstechnologien. Aus sicherheitspolitischer Sicht eröffnen sich daher noch nie dagewesene Vulnerabilitäten auf gesamtgesellschaftlicher Ebene. Das Bewusstsein für jene Verletzlichkeit ist jedoch noch unzureichend in den europäischen Sicherheitsstrategien abgebildet. Angesichts der enormen Geschwindigkeit und Menge an digitalen Informationen und Datenübertragungen verändert sich das Gefahrenpotential: es steigt an und wird zunehmend komplexer. Vor diesem Hintergrund sind Desinformationskampagnen und Cyberangriffe zu den meistverwendeten Waffen der hybriden Kriegsführung und somit zu einer Konstante des europäischen Bedrohungsbilds geworden.

3. Desinformationskampagnen und europäische Maßnahmen im Zuge der COVID-19 Krise

Laut der Weltgesundheitsorganisation kam es im Zusammenhang mit der Ausbreitung der COVID-19 Pandemie zu einem noch nie dagewesenen Ausmaß einer „Infodemie" – die schnelle und weitrechende Ausbreitung schadhafter Desinformation.[9] Dies stellte auch die Europäische Union und ihre Mitgliedsstaaten vor ein neues Maß an Herausforderungen, trotz zahlreicher vergangener Erfahrungen mit Desinformation wie u.a. während dem Brexit Referendum 2016, der französischen „Gelbwesten-Bewegung" 2018 oder im Zusammenhang mit den Wahlen zum Europäischen Parlament 2019.

Desinformation wird von der Europäischen Union klar definiert: Unter Desinformation wird die Erstellung und Verbreitung von nachweislich falschen oder irreführenden Informationen zur beabsichtigten Täuschung der Öffentlichkeit verstanden.[10] Aufgrund der Intention gesellschaftlichen, politischen bzw. ökonomischen Schaden anzurichten beinhaltet die Definition von Desinformation nicht unbeabsichtigte Fehler in der medialen Berichterstattung oder Satirebeiträge. Der Einsatz von systematischen Desinformationskampagnen zielt auf die Spaltung der Gesellschaft ab, indem durch subversive Einflussnahme das Vertrauen in demokratische Institutionen bzw. politische Prozesse ausgehöhlt wird.[11]

Aus der Analyse der Desinformationskampagnen im Zusammenhang mit der COVID-19 Krise geht hervor, dass die Aggressoren hinter jenen Kampagnen gewisse Narrative-Muster[12] verwenden, welche in fünf Kategorien eingeordnet werden können.[13]

1. *„Die EU versagt im Umgang mit der COVID-19 Krise"*: Diese prominente Kategorie an irreführender COVID-19 Desinformation war insbesondere zu Beginn der COVID-19 Krise weitverbreitet. Die Kernbehauptungen besagten, dass sich die EU aufgrund der Krise auflöst und zerfällt. Die erfundenen Falschmeldungen beinhalteten unter anderem Gerüchte, dass mehrere Mitgliedsstaaten die EU verlassen würden und es zu einer Auflösung der Schengen-Zone käme. Jene Narrative zielten direkt auf die Diskreditierung

der EU-Institutionen ab und stellten die Union als völlig handlungsunfähig dar.

2. *„Die EU Mitgliedsstaaten versagen komplett im Umgang mit der Krise“*: Anstatt die EU und ihre Institutionen zur Zielscheibe von Desinformationskampagnen zu machen, richteten sich jene Narrativen gegen die nationalen Regierungen der Mitgliedsstaaten. Einzelne Staaten wurden in ihrem Umgang mit der Krise vollkommen inkompetent und ohnmächtig dargestellt. Obwohl es der Wahrheit entspricht, dass mehrere EU-Länder mit der neuartigen Herausforderung überfordert waren, wurden diese Fakten so weit überspitzt, dass von Staatszerfall, Chaos und Anarchie die Rede war. Dadurch wurde mittels Verblendung und Verzerrung der Tatsachen direkter Einfluss auf die öffentliche Meinung der Bevölkerung genommen, mit dem Ziel den Vertrauensverlust anzufachen.
3. *„Die EU und ihre Mitgliedsstaaten agieren selbstsüchtig und unsolidarisch“:* Während die ersten beiden Narrative den Schwerpunkt auf die angebliche Unfähigkeit der Union und einzelner Mitgliedsstaaten legte, wurde hierbei die vermeintliche Unwilligkeit der europäischen Akteure propagiert. Die verbreiteten Falschinformationen suggerierten, dass einzelne europäische Staaten und Verbündete aus Drittstaaten sowie Partnerländer im Stich gelassen wurden und die europäische Solidarität eine Farce sei. Diese Narrative zielte nicht nur auf den Vertrauensverlust innerhalb der EU ab. Durch die Streuung jener Falschmeldungen in den Ländern der Östlichen Partnerschaft und am Westbalkan wurde versucht, die EU auch über ihre eigenen politischen Grenzen hinweg zu verleumden.
4. *„Russland und China zeigen mehr Solidarität gegenüber den Mitgliedsstaaten als die EU selbst“*: Aufbauend auf den drei ersten Kategorien wurde systematisch der verfälschte Eindruck vermittelt, dass die russische und chinesische Regierung nicht nur besser gegen die Krise gewappnet sei, sondern auch bereitwilliger ihrer Unterstützung anbiete als die EU. Diese falschen Schilderungen wurden mittels perfekt inszenierter Bilder (wie u.a. von russischen Hilfskonvois in Italien) untermauert. Dadurch wurde der Eindruck vermittelt, dass autoritäre Systeme besser mit den Auswirkungen der Pandemie umgehen könnten, während die EU versagt.
5. *„Diverse Narrative“*: Zusätzlich zu den oben genannten Kategorien gab es eine Vielzahl an diversen Narrativen im Zusammenhang mit der Verbreitung und Behandlung des Virus. Diese beinhalteten erfundene Verschwörungsmythen, dass es einen Zusammenhang zwischen der Ausbreitung von COVID-19 und der Ausweitung des 5G-Netzwerks gäbe, oder dass die Verbreitung des Virus in Europa durch Migrant:innen verursacht worden sei. Diese Art von unterschiedlichen Desinformationsfällen nutzt bereits existente und teils polarisierende bzw. emotionalisierte Themengebiete aus und verstärkt soziale Spannungen. Seit der zweiten Jahreshälfte 2020 verbreitete sich Desinformation in Verbindung mit COVID-19 Impfstoffen sowie deren Wirkung im Vergleich zu den anderen Kategorien überproportional stark.[14]

Obwohl die genaue Zuordnung von Desinformation aufgrund der Verschleierung ihrer ursprünglichen Quellen nicht bzw. nur äußerst schwer möglich ist, werden insbesondere Russland und China als Ursprungsländer von Desinformationskampagnen gegen die EU genannt. Aus der Analyse der pro-russischen und pro-chinesischen Narrative kann ein gewisser Konnex abgeleitet werden, der die Intentionen jener Akteure aufdeckt. Hierbei ist speziell seit der Verbreitung von COVID-19-Desinformation eine Veränderung des Trends erkennbar. In der Vergangenheit war die Streuung eindimensionaler Falschmeldungen gängig, welche die EU diskreditiert und chinesische/russische regierungsfreundliche Berichterstattung forciert. Im Zuge der COVID-19 Krise veränderte sich jedoch die Strategie dahingehend, dass multiple Desinformationsnarrative gleichzeitig verbreitet werden, die teils zu einander im Widerspruch stehen. Das Ziel jener neuartigen Taktik, welche eine russische Handschrift trägt und seitens chinesischer Akteure imitiert wird,[15] ist es eine objektive Berichterstattung durch die Überflutung von Unwahrheiten zu untergraben.

Europäische Maßnahmen gegen Desinformation

Zur Untersuchung und Bekämpfung von Desinformation richtete der Europäische Auswärtige Dienst bereits 2015 die Plattform *EUvsDisinfo* ein, um Kampagnen (insbesondere aus Russland) besser vorherzusehen und bei der Entwicklung effektiver Gegenmaßnahmen behilflich zu sein. Aus den Analysen der Aufdecker-Plattform gehen nicht nur die einzelnen Desinformationsfälle hervor, sondern sie beobachtete auch den rasanten Anstieg an COVID-19-Desinfomration. EUvsDisinfo registrierte den ersten Fall von COVID-19-Desinformation Ende Jänner 2020 – Mitte April hatten bereits mehr als 20% aller neuen Desinformationsfälle einen direkten Bezug zu COVID-19.[16]

Einer der jüngsten Meilensteine in der Bekämpfung von Desinformationskampagnen stellt die Annahme der Schlussfolgerung zur EU-weiten entschlosseneren Bekämpfung von hybriden Bedrohungen, insbesondere Desinformation, vom Dezember 2020 dar. Der Europäische Rat verdeutlichte den Handlungsappell, der durch die Desinformationskampagnen im Zuge der COVID-19 Krise verstärkt ins Bewusstsein trat.[17] Die Betonung der Forderungen lag einerseits auf der multidisziplinären Bekämpfung, welche eine Vielzahl von Akteuren umfassen muss, sowie andererseits auf der Stärkung der Task Force für Strategische Kommunikation und des Schnellwarnsystems.[18]

Außerdem sollen die Betreiber von Online-Plattformen, auf denen der Großteil von Desinformation verbreitet wird, vermehrt zu Transparenz und Verantwortung bewogen werden. Vor diesem Hintergrund veröffentlichte die EU Kommission erst vor einem Monat Leitlinien wie der Verhaltenskodex gegen Desinformation gestärkt und zu einem weltweit wirksamen Instrument werden soll.[19] Diese richten sich auch konkret an Plattformen und Soziale Medien, welche u.a. die Finanzierung von Desinformation durch gezielte Werbeeinschaltungen unterbinden sollen. Das übergeordnete Ziel der EU besteht darin, die Verbreitung von Desinformation zu erschweren und die Kosten für ihre Erstellung in die Höhe zu treiben, um sie für Aggressoren unattraktiver zu machen.

Darüber hinaus setzten die EU-Institutionen im Laufe der letzten 12-18 Monate zahlreiche Schritte

Abbildung 2 – Kompass zur Erkennung von Falschmeldung (Quelle: Europäisches Parlament)

und Maßnahmen zur Bewusstseinsförderung, um die Bedeutung der Desinformationsgefahren hervorzuheben sowie die gesellschaftliche Resilienz zu stärken, wie etwa durch die Unterstützung von Faktenprüfer:innen und Forscher:innen.[20] Auf der Ebene der öffentlichen Bewusstseinsbildung rund um die Entlarvung von Desinformation ist der bereits 2019 veröffentliche Kompass zur Erkennung von Falschmeldung (Abbildung 2) nach wie vor ein sehr hilfreiches und anschauliches Mittel.[21]

4. Cyberangriffe und europäische Cybersicherheit im Zuge der COVID-19 Krise

Im Zusammenhang mit der COVID-19 Krise kam es in der EU zu einer deutlichen Zunahme von Cyber-Bedrohungen – von Cyberattacken und Cyber-Spionageaktivitäten bis hin zu Cyberkriminalität.[22] Durch die COVID-19 bedingte Veränderung der privaten und beruflichen Lebensumstände, besonders angesichts der extremen Zunahme an Homeoffice-Tätigkeiten und Online-Shopping aber auch die Digitalisierung von Gesundheitsleistungen, eröffneten sich neue digitale Verletzlichkeiten und Angriffsmöglichkeiten.

Cyberkriminelle und sogenannte Advanced Persistent Threat (APT) Hacker-Gruppen nutzten die neuen Bedienungen aus, um Cyberangriffe auf Behörden, Firmen und Privatpersonen durchzuführen. Neben Phishing-Angriffen kam es zum Missbrauch von speziellen COVID-19 Applikationen und Attacken auf das Gesundheitswesen, bei welchen kritische Daten und finanzielle Mittel gestohlen wurden und es zu gezielten Störungen der Systeme kam.[23] Insbesondere Betrugsversuche durch „Speer-Phishing-Angriffe“ haben während der COVID-19 Krise enorm zugenommen: Analysen zufolge um über 660% im März 2020 im Vergleich zu den Vormonaten.[24] Darüber hinaus zählen der Einsatz von Schadprogrammen, webbasierte Attacken, Spams und Angriffe auf Webanwendungen laut EU zu den größten Cyberbedrohungen 2019 und 2020.[25] Anhand jener Entwicklungen lässt sich eine klare Aussage treffen: Mit dem weltweiten Ausbruch des COVID-19 Virus beschleunigten und intensivierten sich die Bedrohungstrends der Cyberangriffe.[26]

Europäische Cybersicherheitsmaßnahmen

Bereits vor dem europaweiten Ausbruch der COVID-19 Pandemie kam es Mitte 2019 zu einem Durchbruch der Cybersicherheitsmaßnahmen auf europäischer Ebene. Der Europäische Rat etablierte Rahmenbedingungen, um mittels gezielter Maßnahmen auf Cyberangriffe zu reagieren und sie zu verhindern. Um externe digitale Bedrohungen der EU abzuwehren, umfassen jene Instrumente auch „Cyberangriffe gegen Drittstaaten oder internationale Organisationen, wenn restriktive Maßnahmen für notwendig erachtet werden, um die Ziele der Gemeinsamen Außen- und Sicherheitspolitik (GASP) zu erreichen“.[27] Diese Entwicklung stellt einen der wichtigsten Meilensteine in der europäischen Cyberabwehr der letzten Jahre dar.

Mit dem Anstieg der Anzahl und Professionalität der Cyberangriffe seit Beginn der COVID-19 Krise wurde auf EU-Ebene die Notwendigkeit erkannt, schneller und effizienter auf die veränderte Bedrohungslage zu reagieren, um die Integrität und Sicherheit der digitalen Infrastrukturen zu gewährleisten. Infolgedessen beschloss der Europäische Rat Ende Juni 2020 erstmalig restriktive Maßnahmen der Cyber Diplomacy Toolbox in Form von Sanktionen als Reaktion auf Cyberangriffe zu verhängen.[28] Gegen sechs Personen und drei Einrichtungen aus Russland, China und Nordkorea, welche für den versuchten Cyberangriff auf die Organisation für das Verbot chemischer Waffen sowie die als „WannaCry“, „NotPetya“ und „Operation Cloud Hopper“ bekannten Angriffe verantwortlich sind, wurden Einreiseverbote und das Einfrieren von Vermögenswerten verhängt.[29] Ferner erließ der Europäische Rat im Oktober 2020 weitere Sanktionen gegen zwei Personen und eine Einrichtung aus Russland, die an dem Cyberangriff auf den Deutschen Bundestag 2015 beteiligt waren bzw. dafür verantwortlich sind.[30]

Der Hohen Vertreter Josep Borrell verurteile zudem jene Angriffe sowie die erhöhten Cyberbedrohungen im Zuge der COVID-19 Krise scharf, indem er die Angriffe als böswillig, unverantwortlich und destabilisierend bezeichnete.[31] Somit hat sich nicht nur die politische Rhetorik der EU gegen die Aggression, die von Cyberaktivitäten ausgeht, verschärft, sondern auch die damit einhergehenden konkreten Handlungen. Außerdem beschloss der Europäische Rat auf-

grund der anhaltenden Cyber-Bedrohung erst kürzlich, die Rahmen der Sanktionen gegen all jene Personen und Institutionen um ein weiteres Jahr, bis zumindest Mai 2022, zu verlängern.[32] Die Abwehr und Vergeltung von Cyberangriffen wird dadurch immer stärker und unmittelbarer an die Ziele der Gemeinsamen Außen- und Sicherheitspolitik (GASP) gebunden.

Auch auf strategischer Ebene kam es zu maßgeblichen Entwicklungen, als im März 2021 der Europäische Rat die Schlussfolgerungen zur EU-Cybersicherheitsstrategie für die digitale Dekade annahm.[33] Im Kontext des COVID-19 Wiederaufbauplans der EU stellen die Cybersicherheitsmaßnahmen einen essenziellen Beitrag zum Aufbau eines digitalen, widerstandsfähigen und grünen Europas dar und wirken sich daher direkt auf die strategische Autonomie der EU aus. Folgende Aktionsbereiche[34] der Cybersicherheitsstrategie sind von zentraler Bedeutung:

- Erstellung eines **Netzes von Sicherheitseinsatzzentren** in der gesamten EU, um eine verbesserte Überwachung und Früherkennung von Angriffen auf Netzwerke zu ermöglichen
- Etablierung einer **gemeinsamen Cyberstelle** zur Erarbeitung von Cybersicherheit-Schwerpunkten im Rahmen des Krisenmanagements der EU
- Effizienzsteigerung der Instrumente der **EU-Cyberdiplomatie** mit Schwerpunkt auf Präventionsmaßnahmen und Bekämpfung von Cyberangriffen auf Lieferketten, kritische Infrastruktur und demokratische Institutionen/Prozesse
- Engagement für die Implementierung der Maßnahmen des **5G-Instrumentariums** der EU zur Sicherstellung der 5G-Netzsicherheit
- Beschleunigung der Erarbeitung wichtiger **Internetsicherheitsstandards** zur Erhöhung der globalen Internetsicherheit durch allgemeine Standards
- Mögliche Einrichtung einer Arbeitsgruppe für **Cybernachrichtendienste**
- Stärkung der **internationalen Zusammenarbeit** in der Bewusstseinsbildung eines gemeinsamen Verständnisses der Cyberbedrohungslandschaft

5. Conclusio

Die jüngste Intensivierung der hybriden Bedrohungen im Zuge der COVID-19 Krise haben ein Faktum klar verdeutlicht: Desinformationskampagnen und Cyberangriffe treten nicht willkürlich auf, sondern sind das Ergebnis von systematischer und beabsichtigter Einflussnahme durch gezielte Destabilisierung. Vor dem Hintergrund ihrer Komplexität und Intensität haben hybride Bedrohungen im Zuge der COVID-19 Krise ein neues und bislang unbekanntes Maß an Gefahrenpotential erhalten. Cyberangriffe und Desinformationskampagnen, die meistgenutzten Instrumente hybrider Aggression und Subversion, bekommen daher einen größeren Stellenwert im europäischen Bedrohungsbild: sowohl die nachgewiesene Eintrittswahrscheinlichkeit als auch das Schadausmaß sind mit **sehr hoch** zu beurteilen.

Die erläuterten Strategien, Maßnahmen, und Instrumente der EU-Institutionen zur Bekämpfung jener Gefahren (welche keinen Anspruch auf Vollständigkeit haben, sondern nur einen Auszug darstellen) haben sich innerhalb der vergangenen 12-18 Monate stetig weiterentwickelt. Obwohl seitens der EU und ihrer Mitgliedsstaaten heute im Vergleich zu Anfang 2020 ein erhöhtes Bewusstsein sowie verbesserte Gegenmaßnahmen vorhanden sind, sind die Handlungen als **reaktionär** einzustufen. Um ausreichend auf die hybriden Gefahren von morgen gewappnet zu sein, muss die Europäische Union eine **proaktivere** Rolle einnehmen, einschließlich der Etablierung präventiver Schritte und verstärkter Abwehrmechanismen.

Dies kann jedoch nur auf gesamteuropäischer Ebene geschehen und muss eine intensivierte Zusammenarbeit der Mitgliedsstaaten im Sinne der Gemeinsamen Außen- und Sicherheitspolitik inkludieren. Nur so kann die Stabilität und die strategische Autonomie der EU gewährleistet werden, um nicht äußerer Machtausübung zum Opfer zu fallen. Hierbei müssen neuartige, vernetzte Sicherheitsbedrohungen wie dem Einsatz von **Künstlicher Intelligenz**, **Deepfakes** oder **Quantentechnologie** bereits heute mitberücksichtigt werden. Fest steht, dass sich hybride Bedrohungen auch in Zukunft rasant weiterentwickeln und somit die europäische Sicherheit von morgen gefährden werden.

About the Author

Michael Zinkanell, M.A./B.A., ist Stv. 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] ENISA, 2020: „ENISA Threat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected“, Oktober 2020, https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020

[2] ENISA, 2020: „ENISA Threat Landscape 2020 - Main Incidents“, Oktober 2020, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-main-incidents

[3] EUROPOL, 2021: „European Union Serious and Organised Crime Threat Assessment“, April 2021, https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment

[4] KPMG 2021: „Cyber Security in Österreich“ Studie IT Advisory, April 2021, https://home.kpmg/at/de/home/insights/2021/04/cyber-security-studienbestellung.html

[5] Europäische Kommission, 2020: „Coronavirus: EU stärkt Maßnahmen zur Bekämpfung von Desinformation“, Juni 2020, https://ec.europa.eu/commission/presscorner/detail/de/IP_20_1006

[6] Europäische Kommission, 2020: „Coronavirus: EU stärkt Maßnahmen zur Bekämpfung von Desinformation“, Juni 2020, https://ec.europa.eu/commission/presscorner/detail/de/IP_20_1006

[7] Bundesministerium für europäische und internationale Angelegenheiten: “Hybride Bedrohungen” https://www.bmeia.gv.at/themen/globale-themen/hybride-bedrohungen

[8] Herpig, Sven, 2016: “Anti-War and the Cyber Triangle. Strategic Implications of Cyber Operations and Cybersecurity for the State”, Hull University, Jänner 2016, https://www.stiftung-nv.de/de/publikation/anti-war-and-cyber-triangle-strategic-implications-cyber-operations-and-cyber-security

[9] World Health Organization, 2020: „Call for Action: Managing the Infodemic“, 11 December 2020, Statement, https://www.who.int/news/item/11-12-2020-call-for-action-managing-the-infodemic

[10] Europäische Kommission, 2018: „Tackling online disinformation: a European Approach“ COM(2018) 236 final, 26. April 2018, https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2018)236&lang=en

[11] Europäische Kommission, 2019: „Report on the implementation of the Action Plan Against Disinformation“, JOIN(2019) 12 final, 14. Juni 2019, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019JC0012&from=EN

[12] EUvsDisinfo, 2020: “EEAS Special Report Update: Short Assessment of Narratives and Disinformation around the Covid-19 Pandemic” 1. April 2020, https://euvsdisinfo.eu/eeas-special-report-update-short-assessment-of-narratives-and-disinformation-around-the-covid-19-pandemic/

[13] EUvsDisinfo, 2020: “Throwing Coronavirus Disinfo at the wall to see what sticks”, 2. April 2020, https://euvsdisinfo.eu/throwing-coronavirus-disinfo-at-the-wall-to-see-what-sticks/

[14] EUvsDisinfo, 2020: „EEAS Special Report Update: Short Assessment of Narratives and Disinformation around the Covid-19 Pandemic (Update May-November), 2. Dezember 2020, https://euvsdisinfo.eu/eeas-special-report-update-short-assessment-of-narratives-and-disinformation-around-the-covid-19-pandemic-update-may-november/

[15] Axios, 2020: China takes a page from Russia's disinformation playbook“, by Bethany Allen-Ebrahimian, 25 März 2020, https://www.axios.com/coronavirus-china-russia-disinformation-playbook-c49b6f3b-2a9a-47c1-9065-240121c9ceb2.html

[16] EUvsDisinfo, 2020: “Figure of the Week: 8000”, 07. April 2020, https://euvsdisinfo.eu/figure-of-the-week-8000-2/

[17] Europäischer Rat, 2020: „Rat fordert Stärkung der Resilienz und Abwehr hybrider Bedrohungen, einschließlich der Desinformation, im Zusammenhang mit der COVID-19-Pandemie“, Pressemitteilung 15. Dezember 2020, https://www.consilium.europa.eu/de/press/press-releases/2020/12/15/council-calls-for-strengthening-resilience-and-countering-hybrid-threats-including-disinformation-in-the-context-of-the-covid-19-pandemic/

[18] Europäischer Rat, 2021: „Bekämpfung von Desinformation“, https://www.consilium.europa.eu/de/policies/coronavirus/fighting-disinformation/

[19] Europäische Kommission, 2021: „Kommission legt Leitlinien zur Stärkung des Verhaltenskodex für den Bereich der Desinformation vor“, Pressemitteilung 26. Mai 2021, https://ec.europa.eu/commission/presscorner/detail/de/IP_21_2585

[20] Europäischer Rat, 2021: „Bekämpfung von Desinformation“, https://www.consilium.europa.eu/de/policies/coronavirus/fighting-disinformation/

[21] Europäisches Parlament, 2019: „Woran erkennt man Falschmeldungen?“ EPRS | Wissenschaftlicher Dienst des Europäischen Parlaments, Februar 2019, https://www.europarl.europa.eu/RegData/etudes/ATAG/2017/599386/EPRS_ATA(2017)599386_DE.pdf

[22] EUROPOL, 2020: „How COVID-19-related crime infected Europe during 2020“, Report November 2020, https://www.europol.europa.eu/activities-services/staying-safe-during-covid-19-what-you-need-to-know

[23] ENISA, 2020: „Threat Landscape Mapping“, https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/threat-landscape-mapping-infographic-2020

[24] Barracuda, 2020, „Threat Spotlight: Coronavirus-related phishing“, 26.März 2020, https://blog.barracuda.com/2020/03/26/threat-spotlight-coronavirus-related-phishing/

[25] Europäischer Rat, 2020: „Infografik – Cybersicherheit in der EU“, https://www.consilium.europa.eu/de/infographics/cyber-security-in-the-eu/

[26] EUROPOL, 2020: „COVID-19 Sparks Upward Trend in Cybercrime“, 5. Oktober 2020, Press Release, https://www.europol.europa.eu/newsroom/news/covid-19-sparks-upward-trend-in-cybercrime

[27] Europäischer Rat, 2019: „Cyberangriffe: Rat kann jetzt Sanktionen verhängen“, 17. Mai 2019, Pressemitteilung https://www.consilium.europa.eu/de/press/press-releases/2019/05/17/cyber-attacks-council-is-now-able-to-impose-sanctions/

[28] Europäischer Rat, 2020: „EU verhängt erstmals Sanktionen als Reaktion auf Cyberangriffe“, Pressemitteilung 30. Juli 2020, https://www.consilium.europa.eu/de/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/

[29] Europäischer Rat, 2020: „Durchführungsverordnung (EU) 2020/1125 des Rates vom 30. Juni 2020 zur Durchführung der Verordnung (EU) 2019/796 über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen“, https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32020R1125&from=DE

[30] Europäischer Rat, 2020: „Böswillige Cyberangriffe: EU-Sanktionen gegen zwei Personen und eine Einrichtung wegen Hackerangriff auf den Bundestag 2015“, Pressemitteilung 22. Oktober 2020, https://www.consilium.europa.eu/de/press/press-releases/2020/10/22/malicious-cyber-attacks-eu-sanctions-two-individuals-and-one-body-over-2015-bundestag-hack/

[31] Europäischer Rat, 2020: „Erklärung des Hohen Vertreters Josep Borrell im Namen der Europäischen Union zu böswilligen Cyberaktivitäten unter Ausnutzung der Coronavirus-Pandemie“, Pressemitteilung 30. April 2020, https://www.consilium.europa.eu/de/press/press-releases/2020/04/30/declaration-by-the-high-representative-josep-borrell-on-behalf-of-the-european-union-on-malicious-cyber-activities-exploiting-the-coronavirus-pandemic/

[32] Europäischer Rat, 2021: „Cyberangriffe: Rat verlängert Rahmen für Sanktionen um ein weiteres Jahr“, Pressemitteilung 17. Mai 2021, https://www.consilium.europa.eu/de/press/press-releases/2021/05/17/cyber-attacks-council-prolongs-framework-for-sanctions-for-another-year/

[33] Europäischer Rat, 2021: „Entwurf von Schlussfolgerungen des Rates zur Cybersicherheitsstrategie der EU für die digitale Dekade“, Brüssel, 9. März 2021, 6722/21, https://data.consilium.europa.eu/doc/document/ST-6722-2021-INIT/de/pdf

[34] Europäischer Rat, 2021: „Cybersicherheit: Rat nimmt Schlussfolgerungen des Rates zur Cybersicherheitsstrategie der EU an“, https://www.consilium.europa.eu/de/press/press-releases/2021/03/22/cybersecurity-council-adopts-conclusions-on-the-eu-s-cybersecurity-strategy