Gesprächskreis
Nachrichtendienste in Deutschland e. V.

Hybride Bedrohungen gesamtstaatlicher Handlungsfähigkeit

Überlegungen zu ressortübergreifenden Strukturen für die Erfassung, Analyse und Bekämpfung hybrider Bedrohungen

Stellungnahme des GKND

(15.11.2021)

- Hybride Bedrohungen sind seit 2015 in EU und NATO zu etablierten konzeptionellen Begriffen und zum Ausgangspunkt für erhebliche politische wie organisatorische Anstrengungen geworden.
- Strukturen wie die *Hybrid Fusion Cell* im EU INTCEN und der *Hybrid Analysis Branch* im IMS der NATO sind bereits 2016 und 2017 als zentrale, Mitgliedstaaten umfassend einbeziehende bereichsübergreifende Analyse- und Berichterstattungsfunktionen geschaffen und in der Folge schrittweise, wenngleich operativ noch keineswegs vollumfänglich weiterentwickelt worden. Mitgliedstaaten bemühen sich um vergleichbare Strukturen und deren Anbindung an EU und NATO.
- Die Bundesrepublik Deutschland steht hier bisher nicht unbedingt an der Spitze der Entwicklung. Eine klare Zuweisung der nationalen Federführung an das BMI erfolgte erst im Mai 2019. Hybride Bedrohungen werden in interministeriellen konsultativen Foren diskutiert. Eine nationale, ressortübergreifende Stabsstruktur für die Antizipation sowie ggf. zeitnahe Erfassung und Analyse komplexer hybrider Bedrohungen mit institutionalisierten spezifischen Berichtspflichten und -formaten fehlt ebenso wie ihre Entsprechung in ressortübergreifenden Entscheidungsprozessen auf Bund- und Länderebene ebenso wie ihre Konzertation mit EU und NATO. Hierüber kann auch die mutmaßliche Existenz eines „*Aufbaustabes Strategie, Analyse und Resilienz (SAR)*“ nicht hinwegtäuschen.
- Der GKND verdeutlicht im Folgenden erneut die Bedeutung der Thematik und ihrer sachgemäßen Behandlung für die Wahrung vitaler Sicherheitsinteressen Deutschlands und plädiert für einen Neuansatz in der kommenden Legislaturperiode.
- Erste konkrete Überlegungen zu möglichen aufbau- und ablauforganisatorischen Elementen einer leistungsfähigen Struktur werden vorgestellt.

Die Begriffe der hybriden Kriegsführung und der hybrider Bedrohungen haben spätestens seit 2015 einen festen Platz in der Terminologie von NATO und EU und sind Ausgangspunkte für erhebliche organisatorische Investitionen und politische Anstrengungen geworden[1].

Eine zentrale, international allseits geteilte Erkenntnis ist hierbei, dass sich angesichts der Komplexität und Undurchsichtigkeit der Herausforderungen eine wirksame Vorbeugung bzw. Verteidigung gegen hybride Politiken nur durch eine Gemeinschaft gleichgesinnter Staaten mit qualitativ vergleichbaren und vernetzten Befähigungen zu Analyse und Aktion leisten lässt[2].

Alle NATO- und EU-Mitgliedstaaten sind aufgerufen und haben sich seit 2016 in zahlreichen Ratsentschließungen im wohlverstandenen Eigeninteresse auch dafür ausgesprochen, eine effiziente integrierte nationale Abwehr zu organisieren und diese im Bündnis wirksam zu vernetzen[3].

Wo stehen nun die deutschen Bemühungen zur Schaffung adäquater gesamtstaatlicher Strukturen zur Antizipation, zur Detektion, Analyse und Bekämpfung konzertierter hybrider Bedrohungen? Welche konkreten Ansätze müssten auf nationaler und internationaler Ebene in der nächsten Legislaturperiode verfolgt und umgesetzt werden?

Hierauf kann der GKND sicherlich keine umfassende Antwort geben, sieht sich jedoch unter dem Aspekt seines Engagements für ressortübergreifende integrierte Strukturen von Lagefeststellung und Lagebeurteilung als maßgebliche Grundlagen für integrierte Entscheidungen auf politischer und operativer Ebene veranlasst, einige auf praktischen Erfahrungen und Einsichten gründende Überlegungen zu dieser komplexen Frage in die Diskussion einzubringen.

Hybride Bedrohungen

Nach auch in Deutschland etabliertem Verständnis setzen Hybride Bedrohungen voraus[4]:

- Einen (staatlichen/nichtstaatlichen) Akteur, der über geeignete Mittel der verdeckten Beeinflussung/ Manipulation oder des Zwangs unterhalb der Schwelle zur offenen bewaffneten Konfrontation verfügt, und
- der Willens ist, diese in einer Konkurrenz-/Konfliktsituation mit einem anderen (staatlichen/ nichtstaatlichen) Akteur gegen diesen einzusetzen,
- mit dem Ziel, diesen entweder generell zu schwächen, zumeist aber auch, um bei diesem ein bestimmtes, den eigenen Interessen förderliches Verhalten zu bewirken.
- Das Wesen hybrider Maßnahmen ist ganz, zumindest aber in ihrer Urheberschaft verdeckt, um tragfähige Ursachenbestimmung und Attributionen zu vermeiden, hierdurch

[1] Vgl. bereits Major, Claudia und Christian Mölling, Abschreckung plus. Hybride Bedrohungen erfordern eine hybride Sicherheitspolitik, IP, Mai/Juni 2015 (Download)

[2] Zusammenfassend und mit weiterführenden Hinweisen: Bajarūnas, Eitvydas, Addressing Hybrid Threats: Priorities for the EU in 2020 and Beyond, European View 2020, Vol. 19(1) 62 –70 (Download); Szymański, Piotr, Towards greater resilience: NATO and the EU on hybrid threats. OSW Centre for Eastern Studies, Warsaw, 24/04/2020 (Download)

[3] Europäische Kommission. Ein Europa, das schützt: Fortschritte bei der Bekämpfung hybrider Bedrohungen. 29.05.2019 (Download); Gemeinsame Mitteilung an das Europäische Parlament und den Rat. Gemeinsamer Rahmen für die Abwehr hybrider Bedrohungen - eine Antwort der Europäischen Union, 06.04.2016 (JOIN/2016/018 final)

[4] EU2020: Europa im Wettbewerb der Systeme - für mehr Resilienz gegenüber hybriden Bedrohungen, EU-Ministerrat verabschiedet Ratsschlussfolgerungen zu hybriden Bedrohungen, Pressemitteilung BMI 15.12.2020

zusätzliche Desorientierung der Betroffenen zu stiften und negative internationale Konsequenzen bis hin zum Gegenschlag so lange wie möglich hinauszuzögern.

Hybride Maßnahmen sind mithin in der Regel keine Einzelaktionen und auch keineswegs auf ein „tool" wie etwa Desinformation oder *Cyber Network Operationen (CNO)* beschränkt, sondern Teil einer politischen Zielvorstellung, einer Strategie oder eines konkreten Plans unter Einsatz eines breiten Spektrums diverser Mittel und staatlicher wie nichtstaatlicher Akteure. Die gängige Verkürzung des Begriffs „hybride Bedrohung" auf Desinformation ist eine ebenso unzulässige wie potentiell gefährliche Verkürzung ihrer Dimension.

Das Spektrum von Schädigungshandlungen, die im Rahmen hybrider Politik/Kriegsführung zum koordinierten, sich gegenseitig in ihrem Effekt potenzierenden Einsatz kommen können und mithin einer kontinuierlichen Beobachtung und Analyse bedürfen, ist vielfältig, zum Teil unspezifisch, klandestin, dabei aber häufig technisch hochentwickelt und komplex. Es reicht von Propaganda über Desinformation[5], Subversion, Spionage, Sabotage an kritischer Infrastruktur[6] bis hin zur klandestinen Nutzung von Organisierter Kriminalität[7], zur Unterstützung von Sezession und Terrorismus. Ihm muss jeweils fachlich kompetent, koordiniert und reaktionsstark in Erfassung, Analyse und Gegenmaßnahmen begegnet werden[8].

Die rechtzeitige Antizipation, Detektion, Attribution und Neutralisierung hybrider Bedrohungen bedarf mithin eines vergleichbar hohen Grades an Integration und Koordination der Detektions-, Analyse- und Abwehrmaßnahmen und ihrer Träger. Hierbei sind besondere Anforderungen an Zeitgerechtigkeit und Resilienz der beteiligten Strukturen zu stellen, da diese ihrerseits prioritäre Ziele hybrider Maßnahmen (erste Verteidigungslinie) darstellen. Die Bewältigung hybrider Bedrohungen ist damit per se ein klassischer Fall für einen „*Whole of Government Approach*" unter Einschluss weiter Teile von Wirtschaft, Gesellschaft und Wissenschaft[9].

EU Hybrid Fusion Cell und NATO Hybrid Analysis Branch

EU und NATO haben nach den Ereignissen in der Ukraine von 2014 die Herausforderung hybrider Bedrohungen früh aufgegriffen, beschrieben und erste Maßnahmen zu ihrer Bewältigung beschlossen[10].

Am 18. Mai 2015 forderte so der Europäische Rat einen Aktionsplan zur Bewältigung von hybriden Bedrohungen und zur Stärkung mitgliedstaatlicher Resilienz, der im April 2016

[5] Bundesregierung: Desinformation als hybride Bedrohung, (Download)
[6] Freudenberg, Dirk, Hybride Bedrohungen und Bevölkerungsschutz, (Download)
[7] Conrad, Gerhard, Organisierte Kriminalität und hybride Bedrohungen. 01.09.2021, (link)
[8] Vgl. hierzu insbesondere MCDC, Countering Hybrid Warfare Project: Understanding Hybrid Warfare, January 2017, pp. 3-4, 8-10 (Download)
[9] A.a.O., S. 10-15
[10] Zusammenfassend und mit weiterführenden Hinweisen: Bajarūnas, Eitvydas, Addressing Hybrid Threats: Priorities for the EU in 2020 and Beyond, European View 2020, Vol. 19(1) 62 –70 (Download); Szymański, Piotr, Towards greater resilience: NATO and the EU on hybrid threats. OSW Centre for Eastern Studies, Warsaw, 24/04/2020 (Download)

vorgelegt wurde[11] und bereits prominent die Einrichtung einer *Hybrid Fusion Cell (HFC)* im EU INTCEN vorsah[12]:

"Creation of an EU Hybrid Fusion Cell within the existing EU INTCEN structure, capable of receiving and analysing classified and open source information on hybrid threats. Member States are invited to establish National Contact Points on hybrid threats to ensure cooperation and secure communication with the EU Hybrid Fusion Cell".

Im Juli 2016 wurde zwischen EU und NATO in Warschau eine gemeinsame Erklärung unterzeichnet, in der eine Zusammenarbeit auch zur Detektion und Abwehr hybrider Bedrohungen vereinbart wurde[13].

Im Juni 2017 richtete die NATO in der neu strukturierten *Joint Intelligence and Security Division (JISD)* im Internationalen Militärstab Stab der NATO einen *Hybrid Analysis Branch (HAB)* mit vergleichbarer Aufgabenstellung ein[14]. Die Berichterstattung und Analysen des HAB richten sich über den *International Military Staff (IMS)* an den NATO-Generalsekretär, weitere Entscheidungsträger in der NATO wie an die Regierungen der Mitgliedstaaten[15].

Sowohl die EU als auch die NATO haben seither im Rahmen ihrer mitgliedstaatlich bedingten Möglichkeiten erhebliche Anstrengungen unternommen, diese Strukturen auszubauen und operativ zu ertüchtigen[16]. Im Bereich der EU konnte so die *Hybrid Fusion Cell* bereits 2017 auf der Grundlage von *Agreed Terms of Reference* mit der Kommission eine geregelte Zusammenarbeit mit allen Generaldirektoraten einleiten, in deren Zuständigkeitsbereich sich hybride Bedrohungen manifestieren könnten[17]. Über die strukturierten Beziehungen von EU INTCEN und EUMS.INT zu den zivilen und militärischen Nachrichten- und Sicherheitsdiensten der EU-Mitgliedstaaten[18] wie auch über ein schrittweise aufgebautes Netzwerk an *„Points of Contact (PoCs)"* mit den Regierungen[19] konnten Grundlagen für eine Integration der *HFC* in die Kommunikations- und Entscheidungsabläufe geschaffen werden.

---

[11] JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL. Joint Framework on countering hybrid threats a European Union response. JOIN(2016). Brussels, 6.4.2016 (Download)

[12] A.a.O., S. 4

[13] Joint Declaration by the President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organization, Warsaw 16 July 2016 (Download) NATO (Download); EU-NATO cooperation – Factsheet (Download)

[14] Rühle, Michael, Claire Roberts, Enlarging NATO's toolbox to counter hybrid threats (NATO Review, 19.03.2021); NATO's response to hybrid threats, (NATO, 16.03.2021)

[15] NATO International Staff (IS), 04.12.2017 (Download); Joint Intelligence and Security Division JISD (Download), International Military Staff IMS (Download)

[16] Vgl. die zusammenfassenden Darstellungen unter Fn. 10.

[17] EU operational protocol for countering hybrid threats . 'EU Playbook, (SWD 05.07.2021); Vgl. auch EU Commission Defence Industry and Space, Hybrid Threats, (DEFIS 2020); DGAP, The Landscape of Hybrid Threats. A Conceptual Model, 25.02.2021 (Download); Hybrid and cybersecurity threats and the European Union's financial system, Bruegel Policy Contribution (September 2019)

[18] Conrad, Gerhard, Europäische Nachrichtendienstkooperation – Entwicklungen, Erwartungen und Perspektiven, in: Reform der Nachrichtendienste zwischen Vergesetzlichung und Internationalisierung, Mohr Siebeck 2019, 161-177

[19] Conrad, Gerhard, Situational Awareness for EU Decision-making: The Next Decade, European Foreign Affairs Review, Volume 26, Issue 1 (2021) pp. 55 – 70; European Commission, Report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats, Brussels, 28.5.2019 (SWD(2019))

Innerhalb der NATO werden hybride Bedrohungen in den jährlichen *Crisis Management Exercises (CMX)* berücksichtigt; gleiches gilt – im Rahmen der jeweiligen rechtlichen Möglichkeiten – auch für gemeinsame Übungen mit der EU[20].

Unter finnischer wie deutscher Ratspräsidentschaft sind weitere Maßnahmen zur Ertüchtigung der EU-Fähigkeiten beschlossen und eingeleitet worden[21].

Allein dieser nur sehr kursorische Überblick verdeutlicht, dass EU und NATO durchaus erhebliche Anstrengungen unternommen haben, der Herausforderung hybrider Bedrohungen aufbau- und ablauforganisatorisch in konzertierter Lagefeststellung, Lagebeurteilung und Entscheidungsstrukturen gerecht zu werden. Vieles wird auch hier im Detail konkretisierungs- und verbesserungswürdig bleiben, nicht zuletzt auch aufgrund notwendiger mitgliedsstaatlicher Billigung und Unterstützung. Ein sichtbarer Rahmen ist jedoch auf jeden Fall geschaffen worden, an dessen Optimierung gearbeitet werden kann.

Diskussion und Maßnahmen in Deutschland

Im Vergleich zu EU und NATO wirken zumindest die organisatorischen Maßnahmen der Bundesregierung im Hinblick auf hybride Bedrohungen seit 2016 doch eher zurückhaltend, obwohl auch hier bereits von Anfang an kein Zweifel an dem breiten, letztlich einen *„Whole of Government Approach"* bedingenden Spektrum hybrider Bedrohungen bestand[22] und dieses nötigenfalls auch von deutscher Seite öffentlich betont wurde, so zuletzt im Dezember 2020 anlässlich der Verabschiedung von Ratsschlussfolgerungen zum Thema unter deutscher Präsidentschaft[23]:

„Unter hybriden Bedrohungen versteht man die illegitime Einflussnahme durch staatliche oder nichtstaatliche Akteure unter koordiniertem Einsatz verschiedener Methoden (diplomatischer, militärischer, wirtschaftlicher oder technologischer Natur) zur Durchsetzung eigener Interessen, ohne jedoch die Schwelle eines offiziell erklärten Kriegs zu erreichen. Hybride Bedrohungen sind eine Herausforderung, die alle Teile des Staates und der Gesellschaft betreffen. Ziel muss es daher sein, die Resilienz übergreifend und umfassend zu stärken".

Dessen ungeachtet wurde der Diskussions- und Sachstand in der Bundesregierung zur organisatorischen Reaktion auf die hybride Bedrohungslage noch im Mai 2019 in einer Antwort zu

[20] Petrescu, Elena Denisa, Hybrid threats: An avenue for a more solid NATO-EU cooperation (Atlantic Forum, 01.09.2020)

[21] EU vows tougher response on hybrid threats. The pledge follows a rash of reports about hackers targeting hospitals and research institutions. (Politico, 24.07.2020); Fifth Progress Report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats. (European Sources Online, 23.06.2021); Zusätzliche Anstrengungen zur Stärkung der Resilienz und zur Abwehr hybrider Bedrohungen. Schlussfolgerungen des Rates, 10. Dezember 2019 (EU 14972/19) Schlussfolgerungen des Rates zur Stärkung der Resilienz und zur Abwehr hybrider Bedrohungen, einschließlich der Desinformation, im Zusammenhang mit der COVID-19-Pandemie, Brüssel, 15.12.2020 (EU 14064/20)

[22] Tamminga, Oliver, Zum Umgang mit hybriden Bedrohungen. Auf dem Weg zu einer nationalen Resilienzstrategie, 16.11.2015 (SWP-Aktuell 2015/A 92)

[23] Fn. 4

einer Kleinen Anfrage der Fraktion Bündnis90/Die Grünen jedoch wie folgt zusammengefasst[24]:

„[Die Bundesregierung hat] im Jahr 2016 nach der Veröffentlichung der Gemeinsamen Mitteilung des Europäischen Auswärtigen Dienstes (EAD) und der EU-Kommission vom 7. April 2016 und den Schlussfolgerungen des Rates zur Bewältigung hybrider Bedrohungen vom 19. April 2016 hierzu interimsweise ein ressortübergreifendes Netzwerk „Hybride Bedrohungen" eingerichtet. Im September 2018 wurde die ressortübergreifende „Arbeitsgruppe zur Strategischen Koordination des Umgangs mit Hybriden Bedrohungen" geschaffen und das frühere Netzwerk hierein überführt. Seit Juli 2019 hat zudem das Bundesministerium des Innern, für Bau und Heimat (BMI) die ressortübergreifende Federführung für das Thema übernommen. Das BMI setzt im Rahmen der Koordinierung einen regierungsweiten Ansatz um. Demnach sollen alle Ministerien und Behörden in die Abwehr hybrider Bedrohungen eingebunden werden. Hybride Bedrohungen orientieren sich an den Vulnerabilitäten der Gesellschaft und des Staates. Diese begrenzen sich grundsätzlich nicht auf die Zuständigkeit einzelner Ministerien. Im Rahmen des regierungsweiten Ansatzes prüft das BMI auch, ob die bestehenden Strukturen diesem Ansatz gerecht werden".

Dies bedeutet, dass die Europäische Union Anfang 2016 mit der Etablierung der *Hybrid Fusion Cell (HFC)* im EU INTCEN begonnen hatte, gefolgt von der NATO, die im Sommer 2017 einen *Hybrid Analysis Branch (HAB)* in einer neu aufgestellten *Joint Intelligence and Security Division (JISD)* einrichtete[25], während in Deutschland eine erste Federführungszuweisung an das BMI im Mai 2019 erfolgte, ohne dass bis dahin vergleichbare übergreifende organisatorische Strukturen zu handlungsleitender Lagefeststellung und Lagebeurteilung geschaffen worden wären. Bis zum Ende der Legislaturperiode sind auch weiterhin keine fassbaren Ergebnisse der angekündigten Überprüfung bestehender Strukturen „im Rahmen des regierungsweiten Ansatzes", sei es innerhalb des BMI, sei es ressortübergreifend, veröffentlicht worden. Auch die hier zur Verfügung stehende späteste Einlassung der Bundesregierung in ihrer Antwort vom 14.07.2021 auf die Kleine Anfrage der FDP zu Desinformationskampagnen gegen Corona-Schutzimpfungen verweist so unverändert auf die Befassung der „*ressortübergreifenden Arbeitsgruppe zur Strategischen Koordination des Umgangs mit Hybriden Bedrohungen* und in assoziierten Expertengruppen" [26] hin.

Parallel hierzu hat das BMVg mit dem Konzept der vernetzten Sicherheit im Weißbuch 2016[27] und den unter Federführung des AA entwickelten *„Leitlinien der Bundesregierung Krisen verhindern, Konflikte bewältigen, Frieden fördern"*[28] weitere Grundsatzdokumente für integriertes gesamtstaatliches Handeln geschaffen; Ansätze für eine Implementierung in

[24] Aktivitäten der Bundesregierung gegen illegitime Beeinflussung demokratischer Willensbildungsprozesse, Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Dr. Konstantin von Notz, Britta Haßelmann, Agnieszka Brugger, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN (Drucksache 19/11754) (Drucksache 19/12489 vom 19.08.2019), S. 3; siehe auch: Seehofer und die „aktive Cyberabwehr", in: Augen Gerade Aus, 19.05.2019, (download)

[25] Segers, Nico, Enhancing resilience against unconventional attacks on Allied nations: Enter the NATO Counter-Hybrid Support Teams, in: Atlantic Forum, 29.11.2020 (Download)

[26] Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Dr. Jürgen Martens, Stephan Thomae, Grigorios Aggelidis, weiterer Abgeordneter und der Fraktion der FDP (– Drucksache 19/31302 –) BT Drucksache 19/31540 vom 14.07.2021, S. 3, Ziffer 8 (Download)

[27] Bundesministerium der Verteidigung, Weißbuch 2016 zur Sicherheitspolitik und zur Zukunft der Bundeswehr, 13. Juli 2016 (Download)

[28] Die Bundesregierung. Krisen verhindern, Konflikte bewältigen, Frieden fördern, September 2017 (Download)

ressortübergreifend organisierten, verbindlichen handlungs- und entscheidungsrelevanten Strukturen sind jedoch auch hier ausgeblieben[29].

In eigener Zuständigkeit hat das BMVg im April 2017 den Organisationsbereich *„Cyber und Informationsraum (CIR)“* eingerichtet[30]. Auch in diesem wesentlichen Bereich hybrider Bedrohungen wird die Notwendigkeit einer ganzheitlichen ressortübergreifenden Aufstellung betont und in diesem Zusammenhang auf die *„Cyber-Sicherheitsstrategie für Deutschland 2016“* als Handlungsrahmen verwiesen, die bekanntlich noch kurz vor Ende der letzten Legislaturperiode durch eine Fortschreibung ersetzt worden ist[31]. Die dort immerhin enthaltenen allgemeinen Aussagen zur strategischen und operativen Aufgabenwahrnehmung auf Bundes- und Länderebene[32] lassen die Komplexität der aufbau- und ablauforganisatorischen Prozesse allein schon in diesem – wichtigen – Teilbereich hybrider Bedrohungen ebenso erkennen wie die allein schon durch das Ressortprinzip bedingte Notwendigkeit weitergehender stringenter und umfassender Regelungen[33].

Erst im Zusammenhang mit der jüngsten von Belarus im Rahmen eines hybriden Politikansatzes gegen die EU ausgelösten Migrationskrise wird nun am 27. Oktober 2021 in einem exklusiven Medienbericht des Recherchenetzwerks von WDR, NDR und Süddeutscher Zeitung auf einen 2020 geschaffenen *„Aufbaustab Strategie-, Analyse- und Resilienz-Zentrum (SAR)“* und auf dessen bereits im April 2021 erschienenes 19-seitiges Analysepapier *„Szenarien für Migration als Ansatzpunkt hybrider Bedrohungen“* hingewiesen, auf das es jedoch keine politische Reaktion gegeben habe [34]. Ergänzend wird vermerkt, dass an dem Aufbaustab auch AA und BMVg partizipierten, dass dieser auch auf Erkenntnisse von BfV und Bundespolizei zurückgreifen könne, und dass dessen Ziel es sei, „auch innerhalb der Regierung eine Sensibilität für ‚illegitime ausländische Einflussnahme‘ zu schaffen“[35]. Soweit hier erkennbar, ist dies das erste Mal, dass eine solche, offenbar trotz der eindeutig operativen Konnotation des Begriffs *„Aufbaustab“* erneut nur unverbindlich konsultativ-strategische Struktur in der Öffentlichkeit bekannt wird, und dies nur über eine jedenfalls formal unautorisierte Erwähnung, ein angesichts der Bedeutung des Sachverhalts durchaus bemerkenswerter Vorgang.

Soweit auf dieser Grundlage erkennbar, scheinen so zum Ende der vergangenen Legislaturperiode zumindest doch erste Ansätze zu einer spezifischeren ressortübergreifenden Strukturbildung entwickelt worden zu sein, die jedoch erneut über einen rein konsultativ-analytischen Charakter nicht hinauszugehen scheinen und damit bereits deutlich hinter dem immerhin schon einmal operativ ausgerichteten, wenngleich voraussichtlich ebenfalls noch zu straffenden Regelungsniveau der Cyber-Sicherheitsstrategie zurückbleiben.

Angesichts der Komplexität und potentiellen Gefährlichkeit hybrider Bedrohungen und der Dynamik auf EU- und NATO-Ebene, erscheint es daher, wohl nicht nur aus Sicht des GKND,

---

[29] Siehe zuletzt: Bundesministerium der Verteidigung, Hybride Bedrohungen. (Download)

[30] Bundesministerium der Verteidigung. Cyber-Angriffe – Keine Fiktion, sondern Realität (Download)

[31] Bundesregierung. Cybersicherheitsstrategie für Deutschland. (BMI 08.09.2021) (Download)

[32] Cybersicherheitsstrategie für Deutschland 2021 (n. 21), Kapitel 6.4 (S. 19-20)

[33] Vgl. hierzu Stiftung Neue Verantwortung, Deutschlands staatliche Cybersicherheitsarchitektur, 12.10.2021 (Download)

[34] Wenn Menschen zu Waffen erklärt werden. Belarus instrumentalisiert Migranten gegen die EU. Ein Geheimpapier der Bundesregierung warnte schon im Frühjahr vor solchen Methoden. (SZ, 27.10.2021); Flüchtlinge als Druckmittel. Der Diktator von Belarus setzt Flüchtlinge als Druckmittel ein. Schon im Frühjahr warnten deutsche Sicherheitsbehörden in einer Analyse vor genau so einem Szenario. (Tagesschau, 27.10.2021)

[35] Tagesschau (n. 17)

dringlich geboten, einen deutlich energischeren Ansatz in der nächsten Legislaturperiode, vorzugsweise auch in Konzertierung mit der Entwicklung eines Sicherheitsrates, in Angriff zu nehmen. Analytische Bemühungen zur Erfassung von Phänomenologie und Wirkungsweise hybrider Bedrohungen sind zweifellos eine essentielle Grundlage für handlungsleitende Lagefeststellung und Lagebeurteilung, sie können und dürfen jedoch nicht als deren Surrogat dienen.

Ein *Lage- und Analysezentrum* des Bundes?

Die hier vorgestellten Überlegungen zu einem *Lage- und Analysezentrum des Bundes* zu hybriden Bedrohungen können hier allein schon angesichts der zur Verfügung stehenden Quellenlage nur erste Hinweise sein, die dem Ziel einer Identifizierung und Konkretisierung von Ansatzpunkten und Maßnahmen dienen sollen.

Bereits ein erster kursorischer und noch notwendig unvollständiger Überblick verdeutlicht hier die Vielfalt bestehender, auf Bund-/ Länderebene breit gestreuter Potentiale, die es im Interesse einer wirksamen Hybrid-Abwehr zu koordinieren und in leistungsfähige resiliente Melde-, Analyse- und darauf aufsetzende Entscheidungsstrukturen zur Unterstützung der Bundesregierung zusammenzuführen gilt[36]. Die von der Stiftung Neue Verantwortung skizzierten organisatorischen Herausforderungen im Cyber-Bereich[37] stellen sich hier angesichts des Spektrums der mit hybriden Bedrohungen verbundenen Phänomene in noch ausgeprägterer Weise.

Identifizierung, Detektion, Analyse, Attribution und Abwehr von Hybrid Tools & Threats	**Zuständigkeiten – Akteure – Koordinationsbedarf**
Cyber Network Operationen (CNO)	**BMI CI:** NCAZ, BSI, BfV, BKA, **BMVg: Kdo CIR** **BKAmt:** Abt. 7, **BND Abt. TA;** Abt. 6 **BMF:** ITZ Bund
Manipulation von Satellitensystemen (GPS, Galileo, Copernicus)	**BMI BP:** WRLageZ, **BMI KM:** BBK/WRLageZ **BMWi**: DLR/ZKI, ESA, Europäische Kommission **BMVg**: Kdo CIR, WRLageZ
Desinformationskampagnen	**BKAmt**: Bundespresseamt; BND **AA:** Strategische Kommunikation **BMI ÖS:** BfV **BMVg**: BAMAD
Spionage	**BKAmt**: BND **BMI ÖS:** BfV – LfVen **BMVg:** BAMAD
Sabotage	**BMI ÖS:** BfV – LfVen **BMI KM**: BBK **BMVg:** BAMAD

[36] Erstellt auf der Basis der veröffentlichten Organigramme von Bundesregierung und einzelner Ressorts (https://www.bundesregierung.de/breg-de/bundesregierung/bundesministerien mit weiteren Nachweisen)
[37] Fn. 33

Subversion (Unterwanderung/Manipulation von politischen/gesellschaftlichen Gruppierungen)	**BMI ÖS:** BfV – LfVen **BMVg:** BAMAD
Nutzung/Unterstützung von Extremismus als „hybrid tool“ (Subversion)	**BMI ÖS**: BfV – LfVen, **BKAmt:** BND **BMVg:** BAMAD
Nutzung/Unterstützung von Terrorismus als „hybrid tool“ (Subversion)	**BMI ÖS**: BfV – LfVen, **BKAmt:** BND **BMVg:** BAMAD
Nutzung/Unterstützung von Illegaler Migration/Menschenhandel als „hybrid tool“ (Subversion)	**BMI M,** BAMF **BMI ÖS/BP:** BKA, Bundespolizei **BKAmt:** BND
Nutzung/Unterstützung von schwerer Organisierter Kriminalität als „hybrid tool“ (Subversion)	**BMI ÖS:** BKA SO, EUROPOL **BMWI:** **BMF:** ZKA, FIU **BKAmt:** BND
Wirtschaftliche Manipulationen/Pressionen/ Handelskrieg	**BMWI:** BKartA, BAFA, Bundesnetzagentur **BMF:** Bundesbank, FMSA **BMI ÖS:** BKA SO
Finanzpolitische / Währungsmanipulationen/ Währungskrieg	**BMF:** Bundesbank, BAFIN, FMSA **BMI ÖS:** BKA SO
Manipulation/Ausbeutung von Wissenschaft und Forschung (Spionage)	**BMBF** – Länderministerien – Hochschulkonferenz **BMI ÖS**: BfV **BKAmt:** BND
Nutzung, Verschärfung, Auslösung von Pandemien als „hybrid tool“	**BMG** – Länderministerien **BMI KM** – Länderministerien
Einsatz/Verbringung von CBRN	**BMVg:** ABC-Abwehrkommando Bw **BMI KM:** BBK – Länderministerien/behörden
Infiltration/Einsatz/Aufbau paramilitärischer Strukturen	**BMI ÖS/BP:** BKA, BPOL – Länderministerien und Polizeien, BfV/LfVen **BKAmt:** BND (für die Auslandsdimension) **BMVg (ggf.)**

Bereits in dieser notwendig kursorischen Form indiziert diese Übersicht, dass die unabweisbare Grundvoraussetzung für eine erfolgreiche, insbesondere auch zeitgerechte und entscheidungsunterstützende Analyse und Bewältigung komplexer hybrider Bedrohungen eine stabile Aufbau- und Ablauforganisation auf nationaler Ebene mit klar strukturierten, reaktionsstarken Verantwortlichkeiten und synergiefähigen komplementären Kompetenzen ist. Zumindest fachliche und organisatorische Anknüpfungspunkte, wenn nicht sogar klare Zuständigkeiten und Federführungen bestehen hierbei, wenngleich auch ressortintern breit gestreut, für das BMI nahezu im gesamten aufgezeigten Bedrohungsspektrum. Vor diesem Hintergrund ist es ebenso offensichtlich wie naheliegend, dass ein entsprechender Zuweisungsbeschluss der Bundesregierung an das Bundesministerium des Inneren erfolgte[38]. Eher erklärungsbedürftig ist allerdings der

[38] S. oben Fn. 24

Umstand, dass dies erst im Juli 2019 geschah, mithin Jahre nach entsprechenden Entwicklungen in Brüssel, dem man sonst gemeinhin gerne geringe Reaktivität bescheinigt.

Eine derartige Federführungs- und Koordinationskompetenz müsste klar zugewiesen sein, politisch einvernehmlich mit den Ressorts entschieden und in den jeweiligen Geschäftsbereichen samt nachgeordneten Behörden effektiv strukturiert und umgesetzt werden.

Hierzu würde es in der Regel eines förmlichen Regierungs-/Kabinettsbeschlusses, einer unmittelbaren Anbindung des Zentrums an die Entscheidungsebene der Bundesregierung, einer nachhaltigen politischen Begleitung (Prinzip „Chefsache“) und spezifischer Ressortvereinbarungen und Regelungen bedürfen. Wäre eine derartige Struktur nicht ausreichend ausgebildet, in Bund und Ländern akzeptiert, in ihren Verfahren geregelt, erprobt und resilient, würde sie aufgrund der dann inhärent bestehenden Anfälligkeit für Unsicherheiten in den Zuständigkeiten bzw. Kompetenzstreitigkeiten und zeitverzögerten unkoordinierten Gegenmaßnahmen ihrerseits zu einem unfreiwilligen Teil, im schlimmsten Fall zu einem Katalysator gegnerischer hybrider Maßnahmen. Allein schon aus diesem Grund sollte daher eine Integration des Zentrums auf Leitungsebene in nationale, dem Bundeskanzleramt zugeordnete Lage- und Entscheidungsstrukturen angestrebt werden.

Eine solche nationale Struktur, mithin ein „*Hybrid-Lage- und Abwehrzentrum“*, müsste dann wiederum im bilateralen bzw. multilateralen Rahmen mit komplementären Analyse- und Abwehrverbünden gleichgesinnter Staaten und internationalen Organisationen mit dem Ziel koordinierten Vorgehens vernetzt werden.

Ein derartiges Zentrum zur Identifizierung und Abwehr hybrider Bedrohungen auf Bundesebene müsste wiederum aufbau- und ablauforganisatorisch den Spezifika der Bedrohung wie den bestehenden materiellen und strukturellen Rahmenbedingungen in Bund und Ländern Rechnung zu tragen haben:

- Für die einzelnen Bedrohungen (*hybrid threats/tools*) müssten jeweils fachspezifisch qualifizierte thematisch orientierte „*Threat Analysis/Threat Management*“-Arbeitseinheiten (also zu Schädigungsaktionen im/aus dem Cyberraum bzw. Weltraum, Desinformation, Spionage, Sabotage, Subversion etc.) aufgestellt werden, die in der Lage wären, die Bundesregierung zeitnah über sich abzeichnende oder bereits eintretende Aktionen zu informieren, ihre Einordnung in einen breiteren Kontext hybrider Politik eines internationalen Akteurs vorzunehmen, sie in ihrer Relevanz und Gefährlichkeit zu bewerten und Vorschläge für Abwehr- und Gegenmaßnahmen zu unterbreiten.
- Diese Arbeitseinheiten müssten auf der Grundlage der politischen Mandatierung des Zentrums befugt und technisch/organisatorisch in der Lage sein, zur Information der Bundesregierung zeitnah und umfassend auf die Erkenntnisse, Bewertungen und Handlungsoptionen der bereits bestehenden Bund-/Länderkapazitäten zurückzugreifen. Entsprechende Verfahren zur initiativen verzugslosen Meldung und Berichterstattung der zuständigen Stellen an das Zentrum wie auch zur Abfragemöglichkeit durch das Zentrum müssten vereinbart werden. Nur auf dieser Grundlage könnten für die Bundesregierung relevante integrierte Lagebilder erstellt und operative Vorschläge unterbreitet werden.

An die Analyse- und Koordinationsfähigkeit der Arbeitseinheiten wären vor dem Hintergrund der Vielzahl und Verschiedenartigkeit bereits jetzt existierender themenbezogener Akteure in Bund und Ländern mithin hohe Anforderungen zu stellen. Dies gilt umso mehr, als eine der

ersten Aufgaben eine Bestandsaufnahme der bereits geschaffenen oder in Entwicklung befindlichen jeweiligen Analyse- und Operationspotentiale ebenso vorzunehmen sein würde wie eine Identifizierung von Lücken/Schwachstellen und eine Optimierung von Melde- und Berichtswegen sowie eine Strukturierung, Ergänzung und Optimierung der grundsätzlich zur Verfügung stehenden Abwehr- und Gegenmaßnahmen. Der Bundesregierung würde hier eine ständig weiterzuentwickelnde „*anti hybrid tool box*“ zumindest für Standardsituationen zur Verfügung zu stellen sein, über deren Einsatz sie dann nach Lage befinden kann.

Die Arbeitseinheiten müssten mithin von ebenso herausgehobenen wie anerkannten Vertretern der maßgeblichen Behörden in einer Funktion als „Threat Manager (Analysis/Operations)“ geleitet und mit fachkundigem, in den jeweiligen Bereichen gut vernetzten Personal besetzt werden. Hierfür müsste jeder Mitarbeiter des Zentrums in den für seinen Aufgabenbereich thematisch einschlägigen Bereichen in Bund, Ländern, Industrie und Forschung funktional klar identifizierte und über entsprechende Vereinbarungen mandatierte Ansprechpartner (PoCs) haben, die initiativ wie auch auf Anforderung fachliche Hinweise, Erkenntnisse, Warnmeldungen und Analysen zeit- und abnehmergerecht zur Verfügung stellten.

Zur Wahrnehmung seiner Berichterstattungs- und Koordinationsaufgaben würde das Zentrum mit einem technisch leistungsfähigen, in die bestehenden Strukturen der Bundesregierung und auf Bund-Länderebene voll eingebundenen Lagezentrum ausgestattet werden müssen, das seinerseits mit allen einschlägigen Lagezentren auf Bund- und Länderebene (auch im nichtstaatlichen Bereich wie z.B. bei der DLR) sowie in der EU (Kommission, EAD, SATCEN, ESA, ENISA, EUCERT) zu einem geregelten Verbundsystem mit klaren Zuständigkeiten und Abläufen zusammengeschlossen sein müsste.

Auf der anderen Seite dürfte das Zentrum ablauforganisatorisch nicht zum Flaschenhals für die Unterrichtung der Bundesregierung werden. Besonders zeitkritische Erkenntnisse und Warnungen aus den hierfür mandatierten Bereichen müssten im begründeten Ausnahmefall auch direkt an die Entscheidungsträger in der Bundesregierung herangetragen werden können, würden jedoch zeitgleich an das Zentrum zur weiteren Einordnung, Bewertung und Entwicklung von Handlungsoptionen zu übermitteln sein.

Die Kernfunktionen eines derartigen Zentrums sollten damit jedenfalls umfassen:

- Kontinuierliche thematisch strukturierte, hochverdichtete Spitzenberichterstattung an den Bundeskanzler/die Bundeskanzlerin/Leitungsebene Ressorts zu Bedrohungs-potentialen und relevanten Akteuren zur Schaffung eines kontinuierlich angemessenen Niveaus an „*situational awareness*“ und „*preparedness*“.
- Warnmeldungen und dynamische Lageberichterstattung/Analyse im Bedrohungs-/ Schädigungsfall.
- Vorbereitung und Unterstützung der Entscheidungen der Bundesregierung zur Vorbeugung, Abwehr oder Minimierung des schädigenden Ereignisses.
- Fachspezifische Analysen für die zuständigen Bereiche in Bund und Ländern mit dem Ziel der Weiterentwicklung und Verfeinerung des Lageverständnisses und des Aufbaus/der Optimierung angemessener Schutz- und Gegenmaßnahmen.
- Förderung der Ressort- sowie Bund-Länder-übergreifenden Kommunikation und Koordination zwischen den bestehenden Behörden in Lagefeststellung und Lagebeurteilung.

Fazit

Die zunehmende Komplexität und Interdependenz von Herausforderungen und Bedrohungen für unsere Sicherheit erfordert sachgerechte, leistungsfähige und resiliente Lage- und Entscheidungsstrukturen Strukturen auf nationaler wie internationaler Ebene.

Der GKND plädiert dafür, diese dringliche, wenngleich zugegebenermaßen schwierige und komplexe Aufgabe in der kommenden Legislaturperiode ebenso energisch wie pragmatisch und ergebnisorientiert anzugehen, und hofft, mit diesen notwendigerweise nur kursorischen Überlegungen einen Anstoß in diese Richtung geben zu können.

Dr. Hans-Dieter Herrmann
Vorsitzender