„Wie sollten künftige Militärstrategien den sich dynamisch ändernden Herausforderungen im Cyber- und Informationsraum im Rahmen hybrider Kriegsführung begegnen?“

Zusammenfassung Panel 3

General Carl von Clausewitz schreibt im 6. Kapitel des 1. Buches „Vom Kriege“:

> „Ein großer Teil der Nachrichten, die man im Kriege bekommt, ist widersprechend, ein noch größerer ist falsch und bei weitem der größte einer ziemlichen Ungewissheit unterworfen. […] Mit kurzen Worten: die meisten Nachrichten sind falsch, und die Furchtsamkeit der Menschen wird zur neuen Kraft der Lüge und Unwahrheit. In der Regel ist jeder geneigt, das Schlimme eher zu glauben als das Gute; jeder ist geneigt, das Schlimme etwas zu vergrößern, und die Gefährlichkeiten, welche auf diese Weise berichtet werden, ob sie gleich wie die Wellen des Meeres in sich selbst zusammensinken, kehren doch wie jene ohne sichtbare Veranlassung immer von neuem zurück. Fest im Vertrauen auf sein besseres inneres Wissen muss der Führer dastehen wie der Fels, an dem die Welle sich bricht.“

Der preußische General und Strategieexperte kannte weder elektronische Medien, noch „Soziale Netzwerke“, die Nachrichten – wahre oder falsche – in Sekundenbruchteilen weltweit verteilen und damit nahezu ungeheure Wirkung erzielen können.

Jeder Konflikt oder Krieg ist auf seine Weise neuartig und damit wenigstens in Teilen anders beschaffen als die Konflikte oder Kriege zuvor. „Selbst im Verlaufe eines Krieges wandelt sich seine Erscheinungsform fortwährend, das Clausewitz’sche „Chamäleon“ passt sich notwendigerweise den kaum je statischen Gegebenheiten des Kriegsgeschehens an. Damit gesellt sich neben den instrumentellen Gehalt des Krieges, der letztlich ein politischer ist und als solcher, nämlich im Aufzwingen des eigenen Willens, vergleichsweise konstant bleibt, dessen jeweilige geschichtliche Gestalt.“ (Dr. Schaurer: „Alte Neue Kriege – Anmerkungen zur hybriden Kriegsführung“ vom August 2015)

„Wesentliches Merkmal der hybriden Kriegführung ist die Verschleierung eigener Absichten, Fähigkeiten und Handlungen, die, sofern nicht heimtückisch (z. B. ‚false flag‘-Operationen), gemäß Genfer Abkommen, Zusatzprotokoll II Art. 37 von 1977 völkerrechtlich grundsätzlich zulässig ist und damit als fest etabliertes, mithin ‚klassisches‘ Mittel der Kriegführung insgesamt gelten kann.

> „Kriegslisten sind nicht verboten. Kriegslisten sind Handlungen, die einen Gegner irreführen oder ihn zu unvorsichtigem Handeln veranlassen sollen, die aber keine Regel des in bewaffneten Konflikten anwendbaren Völkerrechts verletzen und nicht heimtückisch sind, weil sie den Gegner nicht verleiten sollen, auf den sich aus diesem Recht ergebenden Schutz zu vertrauen. Folgende Handlungen sind Beispiele für Kriegslisten: Tarnung, Scheinstellungen, Scheinoperationen und irreführende Informationen.““ ((Dr. Schaurer, a.a.O.)

Hybride Szenarien und Herausforderungen

Die Palette der „hybriden Szenarien“ erscheint heute gewaltiger als je zuvor. Insbesondere die Fähigkeiten psychologischer Operationen oder operativer Kommunikationsmöglichkeiten zur Beeinflussung der öffentlichen Meinung oder auch gezielt bestimmter Bevölkerungsgruppen verdienen dabei besondere Aufmerksamkeit. Im Zeitalter von „Künstlicher Intelligenz“, „Big Data“ und „Deep Learning“ werden gezielte, gesamtstaatliche Sicherheits- bzw. Abwehr- oder Verteidigungsstrategien und damit koordinierte resiliente Strukturen kritischer Infrastrukturen benötigt.

Das Panel Nr. 3 griff teilweise die Punkte aus dem vorangegangenen Panel Nr. 2 auf und fokussierte seine Betrachtungen auf die Frage „Wie sollten künftige Militärstrategien den sich dynamisch ändernden Herausforderungen im Cyber- und Informationsraum im Rahmen hybrider Kriegsführung begegnen?“

Unter der Leitung von Dr. Martin C. Wolff diskutierten Dr. Florian Schaurer, Referent für Strategieentwicklung in der Abteilung Politik des Bundesministeriums der Verteidigung (BMVg), Fregattenkapitän Dr. Patrick Jungkunz, Referent für Cyber-Politik in der Abteilung Cyber/Informationstechnik des BMVg, und Major i.G. Christian Arendt, Militärischer Assistent des Kommandeurs der NATO Communication and Information Systems Group/Deputy Chief of Staff Cyberspace SHAPE.

Das Panel stützte sich auf eine Definition der „hybriden Kriegsführung“ ab, der eine flexible Mischform von offen und verdeckt zur Anwendung gebrachten regulären und irrregulären, symmetrischen und asymmetrischen, militärischen und nicht-militärischen Konfliktmitteln zugrunde liegt. Diese werden mit dem Zweck zum Einsatz gebracht, die Schwelle zwischen den insbesondere völkerrechtlich so angelegten binären Zuständen Krieg und Frieden zu verwischen.

„Hybride Kriegsführung ist die koordinierte Nutzung militärischer und nichtmilitärischer Mittel, die auf dem Hauptkampfplatz (Main Battlespace) Synergien in physikalischen und psychologischen Dimensionen eines Konfliktes erzielen“ (nach Frank Hofmann: „Conflict in the 21st Century: The Rise of Hybrid Wars“, Arlington VA: Potomac Institute for Policy Studies, 2007).

Hybride Kriegsführung ist insbesondere durch den Einsatz staatlicher Machtmittel unterhalb der Schwelle eines Konflikts mit militärischen Mittel, der die völkerrechtlichen Kriterien eines Krieges erfüllt, gekennzeichnet.

Internationale Aufmerksamkeit hat das Konzept des russischen Generalstabschefs zur „Neuen Generation russischer Kriegsführung“ gefunden. Dieses häufig als „Gerassimow-Doktrin“ bezeichnete Konzept bringt zum Ausdruck, dass politische Ziele nicht mehr allein mit konventioneller Feuerkraft zu erreichen sind, sondern durch einen „breit gestreuten Einsatz von Desinformation, von politischen, ökonomischen, humanitären und anderen nichtmilitärischen Maßnahmen, die in Verbindung mit dem Protestpotenzial der (gegnerischen) Bevölkerung zum Einsatz kommen. Damit verwischt sich sehr deutlich die Grenze zwischen den klassischen Definitionen von Krieg und Frieden.

Die „Gerassimow-Doktrin“ beschreibt im Grunde acht Phasen der hybriden Kriegsführung:

1. Herstellung günstiger politischer, ökonomischer und militärischer Bedingungen für die innere Destabilisierung durch ideologische, diplomatische und wirtschaftliche Operationen sowie Desinformationskampagnen und Methoden psychologischer Kriegsführung.
2. Täuschen und Irreführen der politischen und militärischen Führung des Gegners durch Verbreitung falscher Daten.
3. Aktionen, die dazu führen, dass Regierungsbeamte und Offiziere des Gegners ihre Dienstposten verlassen (einschüchtern, täuschen, bestechen).
4. Verstärkung der Unzufriedenheit in der Bevölkerung (Aktivierung „fünfte Kolonne“, Einschleusen, Subversion).
5. Vorbereiten der militärischen Aktionen (Aufbau Hindernisse, Einschleusung „privater“ Kampfgruppen, Kooperation mit bewaffneter Opposition).
6. Start militärischer Aktionen (nach Aufklärung und Subversion).
7. Vernichtung der Hauptverteidigungskräfte des Gegners durch koordinierte Operationen aller Kräfte einschließlich elektronischer Kampfführung (und Cyber-Operationen)).
8. Zerschlagung übrig gebliebener Widerstandsnester und Zerstörung überlebender Einheiten durch Spezialoperationen.

Suche nach begrifflicher Schärfe

Der Moderator, Dr. Wolff, leitete das Thema mit einer eher philosophischen Betrachtung ein.

Er nannte „hybrid“ als eine unglückliche Beschreibung bzw. eine Beschreibung, die eine sehr spezifische Sichtweise offenbart. Diese Sichtweise nehme eine Trennung zwischen Innen und Außen vor. Stellvertretend könne man es Trennung zwischen Militär und Polizei oder schlicht Gewaltenteilung nennen. Auf jeden Fall sei es eine ganz strikte Trennung. Und wenn jemand irritiert feststelle, dass sich nicht alle an diese Trennung halten, greife man zu einem Begriff und sage, „…da werden zwei Dinge zusammengefügt, die unserem Geschmack nach nicht zusammengehören, nämlich Zivil und Militär oder Polizei und Militär oder kleine grüne Männchen“.

Wenn man sich auf denjenigen einlasse, der das anwende, also jemand, der „kleine grüne Männchen“ losschicke, der brauche den Begriff „hybrid“ nicht. Für den sei es völlig klar, die „kleinen grünen Männchen“ sind phantastische Mittel zur Erfüllung seines (politischen) Zwecks. Zweck und Ziel seien gesetzt und seine Strategie funktioniere.

Weiterhin erwähnte er, dass die begriffliche Trennung vor allem auch aus Gründen juristisch klarer Zuständigkeiten erfolge. Wenn die Zuständigkeit an der einen Grenze ende und an der anderen aber noch nicht anfange, dann gebe es eine Verantwortungsdiffusion. Zugleich wies er darauf hin, dass bestimmte Akteure bewusst die begriffliche Unschärfe oder die definierten Bereiche, für die es keine klaren Verantwortlichkeiten zu geben scheine, für ihre Zwecke nutzten.

Er fügte dann eine Hypothese an, die besagt: „Wir befinden uns mit dem, was wir Digitalisierung nennen, in einem genauso neuen Mix von Begriffen von Konzepten." Hierzu wies er auf Beispiel hin, die zeigen, wie unscharf und wie wenig aussagekräftig häufig verwandte Bezüge auf Strategie oder Taktik im Cyber- und Informationsraum sind und wie komplex sich die Übertragung klassischer Grundlagen und Erkenntnisse zu Sicherheitsstrukturen/-architekturen auf den Cyber- und Informationsraum bzw. Digitalisierung und hybrides Umfeld gestaltet.

Der Cyber- und Informationsraum als „digitales Schlachtfeld"

Im Cyber- und Informationsraum oder – wie gelegentlich verwandt – auf dem „digitalen Schlachtfeld" habe sich das Spektrum der Fähigkeiten, geprägt durch neue Technologien, in einer Weise erweitert, die derzeit noch kaum übersehbar oder hinreichend abzuschätzen sei. Dies erfordere eine ständige intensive Aufklärung der Risiken und Bedrohungen sowie eine hohe Reaktionsfähigkeit bei der Weiterentwicklung und Sicherstellung eigener Abwehr-/Verteidigungsfähigkeiten.

Bei der Planung und Realisierung entsprechender Maßnahmen zur Sicherheitsvorsorge (verwendet wurde u.a. auch der Term „Design in the Battlefield") gelte es u.a. die bisherige strikte Trennung von „Zivil und Militär" oder „Innerer und Äußerer Sicherheit" zu überwinden. Vielmehr seien die Synthese von Körperschaften, von Strukturen sowie von zivilen und militärischen Akteuren herzustellen und die Technologien im Rahmen eines „integrativen Gesamtansatzes" („comprehensive approach") zu nutzen. Der „Vernetzte Sicherheitsansatz" müsse dabei operationell umgesetzt und entsprechende Sicherheitsstrategien angepasst werden.

Bei der Entwicklung und Implementierung eines „integrativen Gesamtansatzes" für die Sicherheit im Cyber- und Informationsraum sind nach Auffassung von Dr. Wolff, neben zivilen und militärischen Kräften der staatlichen Exekutive, auch „Nichtregierungsorganisationen" (NGO) und ggf. sogar „Hacker" als sicherheitspolitische Akteure zu berücksichtigen. Diese müsse man in einer intelligenten Art und Weise zur Gewährleistung hinreichender Sicherheitsvorsorge zusammenbringen. Umfassende Kooperation aller verfügbaren Kräfte zur Gewährleistung effektiver Sicherheit und Verteidigung sei im Cyber- und Informationsraum ein Gebot der Stunde, zumal die entsprechende Expertise und Kompetenz vor allem auch im akademischen und wirtschaftlichen Bereich vorhanden sei und unbedingt genutzt werden sollte.

Hierzu nannte er eine weitere Hypothese, die lautet: „Wenn es stimmt, dass das Konzept von „Design in the Battlefield", also der umfassend vernetzte Sicherheitsansatz im Cyber- und Informationsraum, entscheidend für wirksame Abwehr und Verteidigung gegen Angriffe in dem technologisch global vernetzten Umfeld ist, dann brauchen wir auch zwingend eine gemeinsam getragene soziale, kulturelle oder kommunikative Referenz-Basis."

Spezifische Herausforderungen an Sicherheitspolitik und Strategie im hybriden Umfeld

Dr. Florian Schaurer ging auf die konzeptionellen Grundlagen sowie auf Schwierigkeiten, Herausforderungen und Chancen ein.

Die Bezeichnungen „Hybrid“ und „Cyber“ nannte er unglückliche Worte, weil sie nicht unbedingt beschrieben, was man damit zum Ausdruck bringen wolle. Beide Begriffe seien aber verbreitet und ließen sich politisch operationalisieren. Sie gäben zudem ein grobes Verständnis von der damit verbundenen Instrumenten und Strategien.

Mit Bezug auf einige aktuelle Beispiele aus dem Kontext „hybrider Kriegführung“ stellte er dann konkrete Konsequenzen vor und wies darauf hin, dass die Thematik sicherheitspolitisch u.a. im Weißbuch der Bundesregierung 2016 behandelt werde.

Hybride Bedrohungen seien nicht beschränkt auf den Cyber- und Informationsraum (und nicht auf Russland!), sondern erstrecken sich über sämtliche Lebensbereiche und Politikfelder: Alle und alles können Ziel eines Angriffes werden, insbesondere auch die nicht-militärische Dimension. Schwerpunkt sei die informationelle, psychologische und kognitive Dimension ("Human Domain", Deutungshoheit/ Perzeption, Informationsüberlegenheit).

Das Aufkommen hybrider Aggression sei im Kontext der Renaissance klassischer Machtpolitik und strategischer Einflusssphären zu sehen. Eine - wenngleich verschleierte und dementierbare - staatliche Eskalationsdominanz bleibe Voraussetzung der hybriden Einflussnahme und Kriegführung. Die Selbstbehauptung von Staat und Gesellschaft im hybriden Kontinuum sei daher wesentlich sowohl auf das Verstehen psychologischer Faktoren als auch politisch-strategischer Kalküle angewiesen. Die Abwehr von und der Umgang mit Hybriden Bedrohungen setze ressortgemeinsames und gesamtstaatliches Vorgehen (unter Einbezug des Militärischen) voraus, sie seien DER Anwendungsfall vernetzter Sicherheit. Auch "Nadelstiche" können lähmen und schließlich töten: der Handlungsbedarf ist real und akut - ebenso wie unsere Verwundbarkeit.

Ergänzend führte Dr. Schaurer aus, dass neben der notwendigen Diskussion über Instrumente und Methoden der Sicherheit und Verteidigung im Cyber- und Informationsraum, sich das Augenmerk verstärkt auf den zugrunde liegenden strategischen Anspruch richten müsse. Dies mache tatsächlich einen ganz gravierenden Unterschied. Es mache einen gravierenden Unterschied, ob ein „Cybervorgehen“ aus Gründen klassischer Spionage einfach mit einem neuen Instrumentarium betrieben werde, oder ob sich tatsächlich hinter dieser Konfrontation, die mit hybriden Methoden ausgetragen werde, am Ende des Tages eine Systemkonfrontation verberge, also eine Renaissance klassischer Machtpolitik.

Auf die Fragestellung „warum sind hybride Akteure üblicherweise keine konventionellen Schattenakteure?“ führte Dr. Schaurer aus, dass großen „hybriden Aktionen“, mit denen wir zu tun haben, mit den Nuklearmächten in Verbindung stünden. Deshalb sei die Anwendung „hybrider Aktionen“ im Grunde kein Ausdruck oder Instrument der Schwäche. Die entsprechenden Mächte seinen durchaus in der Lage, Druck oder Zwang zur Durchsetzung ihres Willens in den internationalen Beziehungen mit anderen Mitteln auszuüben. Mittels hybrider Kriegsführung biete sich ihnen jedoch eine Möglichkeit, eigene Absichten, Fähigkeiten und Handlungen zu verschleiern. Hybride Kriegsführung operiere auf höchst kreative Weise größtenteils unterhalb juristisch bestimmbarer Intensitätsschwellen und nehme dem Verteidiger damit die Eindeutigkeit des Reaktionsgrundes.

Als zweiten wichtigen Punkt zu den Kontextbedingungen für hybride Konfliktformen nannte Dr. Schaurer die „Friedensbedingungen“. Das sei eine besonders wichtige Voraussetzung für solche Staaten, die als Verteidiger leichter und schneller unter dem Abwehrregime agieren oder reagieren könnten, als das in Friedensbedingungen (ohne Feststellung eines Spannungs- oder Verteidigungsfalls) möglich ist.

In einem dritten Punkt wurde die „hybride Einflussnahme“ über Informationen angesprochen. Vor allem auch in Kenntnis der jüngsten Erfahrungen dürfe die politische Wirkung von Informationsoperationen nicht unterschätzt werden. Mittels gezielt verbreiterter, insbesondere „geleakter“ (vertraulicher), manipulierter oder sogar bewusst verfälschter Informationen lasse sich die öffentliche Meinungsbildung massiv beeinflussen.

Vor diesem Hintergrund stelle sich u.a. die Frage: „Wie gehe ich mit einem hybriden Akteur um, der gar nicht erst die Bundeswehr im Einsatz angreift, sondern verhindert, dass der Einsatz überhaupt mandatiert wird, indem er auf die öffentliche Entscheidungsbildung, auf die Entscheidungsfindung im Bundestag, in den Gremien, in den einzelnen Parteien Einfluss nimmt, dass dieser Einsatz gar nicht erst mandatiert werden kann?“ Bei Anwendung derartiger Informationsoperationen müsse man die Bundeswehr nicht in einem Einsatzgebiet angreifen; die gewünschte Wirkung könne dann ggf. bereits vorab durch Einwirkung auf den politischen Entscheidungsprozess in Berlin erzielt werden.

Ambiguität im Informationsraum

Vieles davon, was bisher an „Informationsaktivitäten“ festgestellt oder erlebt wurde, sei nicht strafbewährt. Deshalb stelle sich u.a. die Frage „Wo ist der Staat denn zuständig?“ Eine Demokratie müsse u.a. ein gewisses Maß an Ambiguität aushalten. Das bedeute z.B., dass ein nicht unbedingt bestimmungsgemäßer Gebrauch von sozialen Medien toleriert werden müsse. Jeder Bürger habe u.a. das Recht, Unsinn in den sozialen Medien zu verbreiten, wenn die Inhalte keine strafrechtliche Relevanz hätten. Da habe der Staat erst mal nichts verloren. Und er sei auch gut beraten, da nicht einzugreifen. Weil das natürlich eine Ambiguität darstelle, müsse die Gesellschaft das aushalten. Diese sei auch Teil unserer gesellschaftlichen und politischen Resilienz, die darin beruhe, dass man Unterschiede in Meinungen und politischen Haltungen moderieren und ausgleichen könne. Das bedeute letztlich auch eine hinreichende Widerstandskraft und Stärke gegenüber propagandistischer oder gezielt informatorischer Einflussnahme.

Hybrides Vorgehen findet nicht nur gegen Demokratien statt. Demokratien bieten allerdings besonders viele Angriffsflächen durch Vernetzung und Offenheit sowie Transparenz ihrer Strukturen und Prozesse.

Hybride Mittel und Methoden der Konfliktaustragung umfassen grundsätzlich ein breites Spektrum an Instrumenten im zivilen und militärischen Bereich. Die aus der russischen Praxis bekannt gewordenen Instrumente missachten sehr weitgehend rechtsstaatliche Grundsätze und völkerrechtliche Normen.

Konzeptionelle Vorstellungen zur Abwehr und Verteidigung

Die konzeptionellen Überlegungen und Vorstellungen der Bundesregierung zur Abwehr von und Verteidigung gegen hybride Kriegsführung sind im Weißbuch 2016, in der Konzeption zivile Verteidigung (KZV) des BMI sowie in der neuen Konzeption der Bundeswehr (KdB) abgebildet. Diese beiden Dokumente, die KZV und die KdB sollen künftig zusammenfließen in einer Überarbeitung der Rahmenrichtlinien für die Gesamtverteidigung.

Eine gewisse Schlüsselrolle kommt den sogenannten „First Responder" zu, also den Stellen, die in erster Linie mit einem vermutlich hybriden Angriff konfrontiert werden. Das können z.B. Feuerwehr oder die Polizei, aber auch andere zivile oder militärische Institutionen sein. Da solche Angriffe zunächst oder auch grundsätzlich schwer einem Angreifer zuzuordnen bzw. zu attributieren und in ihrem Ausmaß nur schwierig abzuschätzen bzw. zu beurteilen sind, bedarf es einer frühzeitigen und effizienten Beurteilung der Gesamtlage und koordinierten Entscheidungsfindung über Abwehr- oder Verteidigungsmaßnahmen. Ressortübergreifende Koordination und ganzheitliches Handeln sind dabei im Grunde unverzichtbar. Alle wesentlichen Institutionen auf allen relevanten Ebenen von Politik, Exekutivorganen und kritischen Infrastrukturbereichen gilt es in einen ganzheitlich vernetzten Sicherheits-Ansatz einzubinden.

Sicherheit im Cyber- und Informationsraum als gesamtstaatliche Aufgabe

Fregattenkapitän Dr. Patrick Jungkunz widmete sich eines spezifischen Themas der hybriden Kriegsführung und richtete seinen Fokus auf gesamtheitliche, gesamtstaatlichen Cyber-Sicherheit.

Hybride Kriegsführung stelle für den betroffenen Staat vor allem dann eine besondere Herausforderung dar, wenn sie sich unterhalb der Schwelle des bewaffneten Konflikts abspiele. Sie ziele dabei auf alle Bereiche eines Staates und seiner Gesellschaft, im Sinne einer Umkehrung des vernetzten Ansatzes, und ersetze oder komplementiere die klassische Kriegsführung.

In Deutschland werde ein kohärentes staatliches Handeln gegen Aktivitäten der hybriden Kriegsführung vor allem dann erschwert, wenn diese an den Schnittstellen der Behördenzuständigkeiten ansetze. Mit der Wirkung auf die Gesellschaft, insbesondere in Form von politischen, informationellen und wirtschaftlichen Maßnahmen, versuche ein Angreifer grundsätzlich den Rückhalt der Regierung in der Bevölkerung zu schwächen. Darauf richte er in der Regel den Schwerpunkt seiner Aktionen.

Dr. Jungkunz unterstrich, dass zur Begegnung hybrider Bedrohungen sich die zentrale Fragestellung weniger an zukünftige Militärstrategien, sondern vielmehr an die Strategie für eine gesamtstaatliche Verteidigung richten müsse. Ein wichtiger Schritt wäre daher, die Richtlinien der Gesamtverteidigung an das Phänomen einer Kriegführung ohne bewaffnete Auseinandersetzung anzupassen und dabei insbesondere die zivile und militärische Verteidigung aufeinander auszurichten.

Was das Thema hybride Kriegführung betreffe, so sei festzustellen, hinter sich hinter diesem Begriff im Grundsatz nichts wirklich Neues verberge. Operationsführung habe man schon immer mit verschiedensten Mitteln bestritten. Letztlich gehöre das zur „Konzeption der Verbundenen Kräfte", in der alle Mittel der Operationsführung zur Erfüllung des Zweck- und

Ziel-bestimmten Auftrags zusammenarbeiten. Dabei habe man sich immer auch mit Informationen und Informationsoperationen auseinander gesetzt. Missinformationen oder Desinformation sowie Propaganda und gezielte Verbreitung von Gerüchten, Verdächtigungen oder Spekulationen seien auch früher schon in Erscheinung getreten. Zudem habe man elektronische Kampfführung betrieben, also nicht nur mit kinetisch wirkenden Waffen gekämpft, sondern auch mit anderen Mitteln operiert.

Dass neue Mittel, die aus neuen Technologien hervorkommen, in die Operationsführung integriert werden, das sei ein erwartbarer Trend und eine Notwendigkeit hinreichender Verteidigung.

Für ihn seien die bemerkenswerten Aspekte bei der hybriden Kriegführung, dass man diese unterhalb der Schwelle des bewaffneten Konflikts und des bewaffneten Angriffs verwendet, um politische Ziele zu erreichen. Ganz im Sinne wie Clausewitz, der festgestellt habe, „Krieg ist die Fortsetzung der Politik mit anderen Mitteln“. Insofern besetze man bei der hybriden Kriegführung auch sofort den Anschluss an die Politik. Ob man das dann wirklich als Krieg bezeichnen möchte oder nicht, überlasse er den Philosophen an dieser Stelle.

Die jeweils entscheidende Frage sei, ob es sich bei hybriden Operationen um bewaffnete Angriffe im Sinne der völkerrechtlichen Normen oder Aspekte handele. Aus seiner Sicht zeigte sich, dass die hybride Kriegführung entweder komplett losgelöst von Kampfhandlungen stattfinde und in diesem Sinne die klassische Kriegführung ersetze oder, dass sie die klassischen Kampfhandlungen ergänze und in diesem Sinne auch das Gefechtsfeld erweitere. Dabei ziele hybride Kriegführung grundsätzlich auf alle Bereiche von Staat und Gesellschaft. Damit ergäben sich natürlich auch durch die Vernetzung und die Digitalisierung neue Möglichkeiten, strategisch und operativ Erfolge zu erzielen, z.B. bei Einflussnahme durch soziale Netzwerke. Und die weite Verbreitung der sozialen Netzwerke helfe hier natürlich die Reichweite und die Erfolgsaussichten deutlich zu erhöhen im Vergleich zu den Mitteln, die man früher zur Verfügung hatte.

Mit den bereits heute verfügbaren Cyber-Mitteln könne man auf Distanz und zudem skaliert sowie ggf. sehr niedrigschwellig agieren. Das erlaube in gewissen Grenzen jeweils eine Kontrolle des Eskalationsrisikos. In aller Regel arbeite man nicht letal; in aller Regel entstünden auch keine menschlichen Schäden. Er glaube, es sei auch noch nicht bekannt, dass mit Cyber-Mitteln wirklich menschliche Schäden direkt hervorgerufen worden seien. Ebenfalls seien die mittelbaren Schäden, die sich aus Cyberoperationen ergeben hätten, waren nie so groß gewesen, dass sie überhaupt mediale Aufmerksamkeit erregt hätten. Und, man könne damit hervorragend verdeckt arbeiten. Außerdem seien der Kreativität natürlich keine Grenzen gesetzt, um unterhalb der Schwelle des bewaffneten Angriffs politische Ziele zu verfolgen.

Attribuierung als zentrale Herausforderung

In all den bekannten Fällen habe die Attribuierung große Schwierigkeit bereitet. Zudem hätten die vermutlichen Akteure jeweils die Möglichkeit gehabt, die Tat abstreiten zu können. Dies habe es dann wiederum den betroffenen Staaten sehr viel schwieriger gemacht, auf politischer

Ebene überhaupt eine Entscheidung zu treffen und auf Angriffe mit wirksamen Verteidigungs- oder Gegenmaßnamen zu reagieren.

In diesem Zusammenhang fügte Dr. Jungkunz noch an: Attribuierung sei letztlich auch eher ein politisches Mittel. Attribuierung werde häufig vor allem als forensische oder als technische Maßnahme gesehen. Dies gehe dem Ganzen sicherlich voraus. Aber letzten Endes sei es eine Frage des politischen Willens eines Staates, gegen Angriffe mit aus seiner Sicht geeigneten Maßnahmen und Mitteln vorzugehen. Wenn ein Staat entsprechend auf Angriffe antworten möchte, dann würde er auch versuchen, den Angreifer zu identifizieren und zu benennen, oder er würde es aus politischen Gründen bewusst unterlassen, mit dem Finger auf den vermeintlichen Täter zu zeigen. Das könnte im beispielsweise eher die Nutzung diplomatischer Prozesse oder Kanäle zur Problemlösung ermöglichen.

Verteidigung im hybriden Umfeld des Cyber- und Informationsraums als integraler Bestandteil der Gesamtverteidigung

Bezogen auf Deutschland, sei es bisweilen schwierig, notwendige Sicherheitsvorkehrungen oder Abwehr-/Verteidigungsmaßnahmen gegen Aktivitäten der Kriegsführung im Allgemein und der hybriden Kriegsführung im Besonderen umzugehen, insbesondere, wenn dabei überlappende Zuständigkeiten zwischen den zivilen Exekutivorganen und der Bundeswehr in Erscheinung treten. Dies erschwere dann das eigentlich notwendige Zusammenwirken im verbundenen Ansatz und letztlich ein kohärentes staatliches Handeln.

Im Allgemeinen versuche man diese Probleme in verschiedenen Bereichen durch nationale Sicherheitszentren bzw. nationale Abwehrzentren zu lösen, wie z.B. das „Nationale Lage- und Führungszentrum Sicherheit im Luftraum“, das „Weltraum-Lagezentrum“ das „Nationale Cyber-Abwehrzentrum“.

Aus seiner Sicht sei das „Center of Gravity“ der Rückhalt der Regierung in der Bevölkerung. Ohne den Rückhalt der Regierung in der Bevölkerung werde keine Regierung agieren können. Unter den Gegebenheiten werde man genau auf diesen Rückhalt in der Bevölkerung achten. Das mache man politisch mit informationellen Mitteln, mit wirtschaftlichen Maßnahmen oder auch mit infrastrukturellen Maßnahmen. Dementsprechend müsse man damit rechnen, dass Angreifer sich auf kritische Infrastrukturbereiche konzentrieren, und ggfs. die Energie-, Wasser-, Gesundheits- oder Lebensmittelversorgung stören oder sogar unterbinden. Parlament, Regierung und staatliche Verwaltungen könne man zudem unter Druck setzen durch gezielte Verbreitung von Desinformation, mit denen die Bevölkerung verunsichert oder aufgewiegelt wird und somit die letztlich auch die politische Situation entscheidend beeinflusst wird.

Wichtig sei festzustellen, dass, solange die Schwelle des bewaffneten Konflikts nicht überschritten werde, sei das Ganze zunächst keine Frage des Militärs darstelle. Aus seiner Sicht sei es vielmehr eine Frage der Strategie zur Gesamtverteidigung. Die Cyber- und Informationssicherheit stelle einen Schwerpunkt der Gesamtverteidigung dar. Man brauche einen wirklichen vernetzten Sicherheitsansatz. Dazu gehörten die bereits erwähnten Abwehrzentren, aber auch eine effiziente ressortübergreifende Koordinierung zwischen allen Sicherheitsorganen und Sicherheitseinrichtungen.

Abschließend wies Dr. Jungkunz auf die Bedeutung Sicherheitsbewusstsein aller Bürgerinnen und Bürger eines Staates sowie auf die Aus- und Weiterbildung in Angelegenheiten der Cyber- und Informationssicherheit. Er unterstricht die Notwendigkeit, bereits in den Schulen einen kritischen Umgang mit Informationen zu vermitteln. Letztlich sei die Gewährleistung von Cyber- und Informationssicherheit im hybriden Umfeld eine gesamtstaatliche Aufgabe.

Militärstrategie der NATO

Major i.G. Dipl.-Ing. (FH) Christian Arendt wies in seinen Ausführungen u.a. auf die Anerkennung des Cyber- und Informationsraums als Dimension der Operationsführung („Cyberspace as a Domain of Operations“) auf dem Gipfel von Warschau 2016 hin. Damit habe die NATO den ersten Schritt gemacht, diese Dimension in ihre Überlegungen für zukünftige Strategien mit einzubeziehen. Dazu gelte es natürlich den „Cyberspace“ zu definieren und aus Sicht der Allianz auch eine entsprechende Befähigung aller 29 Mitgliedsstaaten des Bündnisses zu fordern. Dies sei mit dem „Cyber Defense Pledge“ begonnen worden. Hierzu unterstrich er die rein defensive Ausrichtung der Cyber-Verteidigungsfähigkeiten in der Allianz.

Unter Berücksichtigung diverser Aspekte der Einzigartigkeit des „Cyberspace“ (u.a. Einfachheit des Zugangs, geringere Hemmschwellen, erschwerte Lokalisierung des Ausgangspunktes, Globalität des Mediums) könne das Ziel unter zwei Gesichtspunkten beschrieben werden:

- Die NATO ist befähigt sich selbst im Cyber und Informationsraum so zu verteidigen, wie zu Land, in der Luft und zur See.
- Der Cyber- und Informationsraum ist vollständig in die multi-dimensionäre Planung der Allianz und all ihrer Mitglieder eingebunden.

Dieses Ziel mit den entsprechenden Mitteln, Kräften und Verfahren zu erreichen, das bedinge die Akzeptanz folgender Thesen:

- Im Rahmen der hybriden Kriegsführung ist im Zeitalter der vernetzten Operationsführung jeder ein potentielles Ziel. Eine 360 Grad Betrachtung ist zwingend Notwendig, um einer etwaigen Bedrohung zu begegnen. Verlust sensibler Informationen wiegt schwerer als die Nichtverfügbarkeit von Kommunikationsmitteln.
- Die Koordinierung von Effekten im Cyberspace erfolgt am besten zentralisiert, permanent und in einem hohen Bereitschaftsgrad schon vor dem Zustand von Krise oder Konflikt.

In seinen Ausführungen stellte Arendt die Aspekte einer Militärstrategie der NATO mit integrierten Cyberverteidigungsfähigkeiten in den Mittelpunkt. Dabei begann er mit einer Bestandsaufnehme:

Der NATO Gipfel in Warschau 2016 habe den Cyberspace als eigene Dimension neben Land, Luft, See in der NATO festgesetzt (s.o.). Dementsprechend sei dann in Vorbereitung auf den Gipfel dieses Jahr in Brüssel ein Aktionsplan mit der Bezeichnung „Implementation of Cyberspace: A Roadmap to Resilience“ erstellt und verabschiedet worden. Beim NATO

Gipfel in Brüssel, im Juli 2018, sei zudem die Aufstellung des Cyberspace Operation Centers im Bereich SHAPE, beschlossen worden.

Ein zentraler Baustein sei ebenfalls die im ersten Quartal 2018 vom NATO-Rat beschlossene „MILITAIR DEVISION AND STRATEGY FOR CYBERSPACE AND DOMAINS OPERATIONS“. Diese enthalte u.a. eine Beschreibung des „Cyberspace“ aus Sicht der Allianz, als eigene Dimension der Operationsführung, in der gleichrangig zu und neben den Domänen Land, Luft und See agiert werde. Allerdings besitze der Cyberraum eine besondere funktionale Dimension, die ganz klare Schnittstellen zu den drei klassischen Dimensionen mit einigen Spezifika aufweise, wie z.B. Globalität, Durchdringung aller Bereiche, breites Funktionsspektrum und besondere Verwundbarkeit.

Hinsichtlich der Absicherung im hybriden Umfeld des Cyberraums bestünden besondere Herausforderungen. Einerseits böte die Isolation von Systemen größtmöglichen Schutz. Alles was man abschlösse oder abschotte, böte keine unerlaubten Zugangsmöglichkeiten für Eindringversuche. Auf der anderen Seite sei aber der erforderliche Informationsaustausch zur umfassenden Informationsversorgung für eine ganzheitliche und hinreichend verlässliche Lagedarstellung und Lagebeurteilung zwingend notwendig, auch um den Schutz aller eigenen Kräfte zu gewährleisten. Allerdings biete jede Schnittstelle auch Sicherheits-Schwachstellen und dementsprechend Eindringmöglichkeiten.

Eine künftige Militärstrategie müsse gewährleisten, dass die Cyberdomäne als vollwertige Domäne neben Land, Luft und See Berücksichtigung finde sein und vollständig, multidimensional in den militärischen Planungsprozess eingebunden werde.

In der nachfolgenden Diskussion mit dem Auditorium wurden u.a. folgende Themen und Aspekte behandelt:

- Zusammenarbeit NATO und EU im Bereich der Cybersicherheit: Grundlegendes Ziel ist eine sich komplementär ergänzende Zusammenarbeit.
- Definition der Begriffe Verteidigungsfall und Spannungsfall im Kontext des Cyber-und Informationsraums: Verfassungsrechtlich sind beide Dinge abgedeckt durch Artikel 87a Grundgesetz. D.h. in diesem Kontext können wir unsere Streitkräfte einsetzen, natürlich unter den Rahmenbedingungen Parlamentsbeteiligungsgesetzt und den damit verbundenen Regelungen.
- Aktive bzw. offensive Cyberverteidigungs-Fähigkeiten: Die NATO verfügt über eigene Fähigkeiten der passiven Verteidigung. Hinsichtlich offensiver Verteidigungsfähigkeiten muss sich die NATO grundsätzlich auf Fähigkeiten einzelner Mitgliedsnationen abstützen, die der Allianz entsprechende offensive Fähigkeiten anbieten und zur Verfügung stellen.
- Zivil-militärische Zusammenarbeit im Cyberbereich: Hierzu wurde die Bedeutung der Kooperation zwischen staatlichen Stellen und der Industrie sowie anderen zivilen Stellen unterstrichen.
- Risiken und Bedrohungen durch Informationsoperationen über Smartphones und „soziale Netzwerke“: In der Antwort wurde insbesondere die Bedeutung und Notwendigkeit von Methoden/Verfahren zur Erkennung von Informationsoperationen mit

falschen/gefälschten Informationen und von effektiven Abwehrstrategien unterstrichen. Außerdem wurde auf den hohen Wert von Aufklärung und Transparenz nach rechtsstaatlichen Prinzipien hingewiesen.

- Überschneidung von innerer/äußerer Sicherheit im Cyber-und Informationsraum und Bewertung der Zusammenarbeit verantwortlicher staatlicher Stellen: Die Panellisten verwiesen auf die eingeleiteten Maßnahmen der zuständigen Ressorts, u.a. Erweiterung des Nationalen Cyberabwehr-Zentrums und Aufstellung des Kommandos Cyber- und Informationsraum.

Fazit

Insgesamt wurde vor allem die Notwendigkeit einer Strategie für gesamtstaatliche Verteidigung hervorgehoben und dabei eine künftig noch stärkere Ausrichtung auf intensive zivil-militärische Verteidigung gefordert.

Da im Rahmen hybrider Kriegsführung und im Zeitalter der vernetzten Operationsführung jedes Individuum und sämtliche Lebensbereiche sowie Politikfelder potenzielle Ziele von Angriffen sein können, darf künftig im Cyber- und Informationsraum nicht auf eine permanente Abwehrbereitschaft und Verteidigungsfähigkeit verzichtet werden.

Die Selbstbehauptung von Staat und Gesellschaft im hybriden Umfeld unterliegt dabei nicht nur politisch-strategischen sowie technologisch-strategischen Faktoren, sondern in zunehmendem Maß auch psychologischen Faktoren. Letztere erhalten angesichts der Allgegenwart und den dynamisch wachsenden Fähigkeiten moderner Medien, insbesondere auch der „Sozialen Netzwerke“, einen unvergleichlich hohen Stellenwert. Die erfolgreiche Abwehr von und der Umgang mit den heutigen und künftigen vermutlich noch zunehmenden Hybriden Bedrohungen setzen ressortgemeinsames und gesamtstaatliches, zivil-militärisches Vorgehen voraus.

Zum Autor: Generalleutnant a.D. Dipl.-Inform. Kurt Herrmann fasste das Panel zusammen.