**Editorial**

zum

**Sammelband**

über die

**52. Sicherheitspolitische Informationstagung**

zum Thema

**„Strategie im 21. Jahrhundert unter besonderer Berücksichtigung moderner technologischer Entwicklungen:**
**Welche Herausforderungen stellen künstliche Intelligenz und autonome Systeme an Politik, Gesellschaft und Streitkräfte?“**

Der preußische General, Militärreformer und Strategieexperte Carl Phillip Gottlieb von Clausewitz hat in seinem Hauptwerk „Vom Kriege“ den Krieg als Instrument der Politik ausführlich analysiert. Die Wahl der geeigneten Mittel sowie des rechten Maßes der Mittel für die Gewaltanwendung, um einen Gegner zur Erfüllung unseres Willens zu zwingen, bestimmt nach Clausewitz als Kern einer Strategie die Möglichkeiten des Handelns. Seit Clausewitz‘ Zeiten hat sich die Palette militärisch nutzbarer Mittel erheblich erweitert. Auch deshalb bedarf es einer zeitgemäßen Interpretation seiner Erkenntnisse. Unter dieser Prämisse ist es nach wie vor sinnvoll, dass sich politische und militärische Entscheidungsträger mit Clausewitz‘ Prinzipien und Methoden auseinandersetzen und sie bei der Beurteilung der Lage, Definition des Zwecks militärischer Einsätze und Festlegung strategischer Ziele für entsprechende Missionen beachten.

Vor allem die aktuelle Diskussion zum Einsatz bewaffneter Drohnen und „autonomer Systeme“ hat den Blick auf die modernen technologischen Entwicklungen, die für die Ausrüstung der Streitkräfte relevant sind, wieder in den Fokus breiter Gesellschaftskreise gelenkt. Moderne Werkstoffe, Nanotechnologie, hochauflösende Sensorik und allgegenwärtige Digitalisierung haben die Herstellung leistungsfähiger automatisierter Systeme mit zunehmend auch autonomen Fähigkeiten ermöglicht. Die Technologien des Cyber- und Informationsraums durchdringen heute alle Lebensbereiche. Umfassende Vernetzung, superschnelle Übertragungskanäle, komplexe Speicher- und Prozessortechnologien für „Big Data“ und „Künstliche Intelligenz“ haben die Fähigkeiten moderner Systeme in nahezu ungeahnter Weise gesteigert. Damit wurden jedoch nicht nur neue, erheblich ausgeweitete strategische, operative und taktische Möglichkeiten geschaffen, sondern zugleich auch neue Risiken und Verwundbarkeiten erzeugt. Darüber hinaus sind vielfältige, teilweise höchst komplizierte Fragen zu Konsequenzen für die Sicherheitspolitik sowie zu ethischen, völkerrechtlichen, soziologischen, personellen und wirtschaftlichen Aspekten entstanden.

Mit solchen Themen und Fragen befasste sich die 52. Sicherheitspolitische Informationstagung. Diese Tagung fand vom 22. bis 24. August 2018 erneut als gemeinsame Veranstaltung der Clausewitz-Gesellschaft e.V. und der Führungsakademie der Bundeswehr im Manfred-Wörner-Zentrum der Clausewitz-Kaserne in Hamburg statt. Im Mittelpunkt der Vorträge und Diskussionen standen insbesondere die Möglichkeiten, Chancen und Risiken disruptiver Technologien oder technologischer Quantensprünge und vor allem die damit verbundene "dritte waffentechnische Revolution“. Neben den potentiellen Anwendungen der Technologien und deren sicherheitspolitischen sowie militärstrategischen Auswirkungen wurden ebenfalls Möglichkeiten zur Rüstungskontrolle, Vertrauensbildung sowie Einhaltung völkerrechtlicher und ethischer Normen untersucht. Einen Schwerpunkt bildete dabei das Bemühen um frühzeitige

Überlegungen und Maßnahmen zur notwendigen Kontrolle und Beherrschung der sich abzeichnenden Entwicklungen.

Der vorliegende Sammelband enthält Beiträge zu wesentlichen Inhalten der Vorträge und Diskussionen der 52. Sicherheitspolitischen Informationstagung.

Den Gastvortrag beim festlichen Abendessen hielt der Präsident des Bundesamtes für Sicherheit in der Informationstechnik, Dipl.-Betriebswirt Arne Schönbohm, zum Thema „Cyber-Sicherheit als Gemeinschaftsaufgabe - wo stehen wir heute und welche Herausforderungen gilt es zu bewältigen?“ Ausgehend von einer Bewertung der Gefährdungslage bezeichnete er IT-Sicherheit als eines der zentralen Themen der Informations- und Kommunikationstechnologie. Dazu nannte er zentrale Forderungen zur Gewährleistung der entsprechenden Sicherheit und ging auf die dazu bereits vorhandenen und auch auf die künftig vorgesehenen Strukturen und Fähigkeiten ein.

Eine außerordentlich Gedanken anregende ökumenische Morgenandacht hielt Militärdekan Dr. Hartwig von Schubert zum Thema „Der Sündenfall im Cyber Age“.

Den inhaltlichen Aufschlag platzierten sehr treffsicher der investigative Journalist und Buchautor Jay Tuck sowie Professor Dr. Dr. Michael Lauster, der Leiter des Fraunhofer-Instituts für Naturwissenschaftlich-Technische Trendanalysen.

Den Einstieg in die Thematik KI setzte Jay Tuck, Für ihn sei KI nach dem Buchdruck die wichtigste Erfindung in der bisherigen Menschheitsgeschichte, stellte Tuck einführend fest. Noch stehe sie am Anfang ihrer Entwicklung, aber bald schon könnte sie „wie ein Tsunami über die Menschheit rollen“. Ihr Entwicklungspotential sei ungeheuer und werde der Menschheit voraussichtlich große Chancen und Innovationsmöglichkeiten eröffnen; zugleich aber würden bei vielen Menschen Ängste hinsichtlich eines möglichen Kontrollverlusts über die weitere Entwicklung geweckt. Schon jetzt dringe intelligente Software immer tiefer in Aufgabengebiete ein, die früher menschlichen Spitzenkräften vorbehalten waren. In wenigen Jahren könne KI weite Bereiche unseres Lebens kontrollieren, und irgendwann entstehe die Gefahr, dass sie sich verselbstständige und in eine „Evolution ohne uns“ einmünde.

Univ.-Professor Dr.-Ing. Dr. rer. pol. habil. Michael Lauster kleidete seinen Vortrag zum Thema „Künftige Technologien und technologische Quantensprünge mit erwarteter Relevanz für Sicherheitspolitik und Strategie“ in eine fesselnde Rahmengeschichte. Er stellte das hohe Entwicklungspotential „Künstlicher Intelligenz“ (KI) dar, ging auf die mit dieser Technologie verbundenen Risiken ein und sprach etliche Konsequenzen potentieller Anwendungen an, die in den später nachfolgenden Diskussionen und Panels vertiefend behandelt wurden.

Die Gesprächsrunde mit Jay Tuck und Prof. Dr. Michael Lauster wurde vom Moderator, Prof. Dr. Holger M. Mey, mit sieben Thesen zum Einfluss künftiger disruptiver Technologien auf Sicherheitspolitik und Strategie eröffnet. Die Diskussion konzentrierte sich sehr stark auf das breite Spektrum der Aspekte zu KI und Systemen mit autonomen Fähigkeiten. Weitere Kernpunkte der Diskussion waren z.B. Herausforderungen durch neuartige Risiken und Gefährdungen infolge moderner, disruptiver Technologien, Gewährleistung menschlicher Kontrolle über künftige Systeme, Fragen zur ethischen Dimension von Waffensystemen mit autonomen Fähigkeiten, zur Proliferation von sensitiven Technologien, zu völkerrechtlichen Konsequenzen, zu Möglichkeiten von Rüstungsbegrenzung, Abrüstung und Vertrauensbildung,

aber auch zur Gewährleistung hinreichender Resilienz von gesellschaftlichen, politischen und staatlichen Strukturen. Diese Themen zogen sich dann wie ein roter Faden durch die gesamte Tagung.

Ein von Teilnehmern des Lehrgangs Generalstabs-/Admiralstabsdienst National (LGAN) 2017 durchgeführtes „Spezial-Panel“ untersuchte „Welche Auswirkungen auf die Militärstrategie sind durch Künstliche Intelligenz (KI) und Autonomer Waffensysteme zu erwarten?“. Hierbei präsentierten die Panellisten (Oberstleutnant Kristof Trier, Flottillenarzt Dr. Elisabeth Brunn, Major Markus Levy, Major Maik Schröder und Major Mike Dunn (US)) sowie die beiden Moderatoren (Korvettenkapitän Patrick Jacobi und Major Benedikt Kühn) ihre Überlegungen in einem ganzheitlichen Sicherheitsansatz und stellten zuvor erarbeitete Thesen zur Diskussion. Weitgehend unbestritten waren die Erwartungen an moderne Technologien, soweit sie zu einer Stärkung der menschlichen Leistungsfähigkeit (Human Performance Enhancement, HPE) beitragen können. Hinsichtlich erwartbarer autonomer Fähigkeiten wurde wiederholt die Forderung nach Einhaltung ethischer Normen unterstrichen und die Notwendigkeit zur Festlegung und Beachtung völkerrechtskonformer Einsatzmodalitäten und Verhaltensregeln (Code of Conduct) begründet.

Das Panel 2 (Generalmajor Dipl.-Inform. Jürgen Jakob Setzer, Stellvertretender Inspekteur des Kommandos Cyber- und Informationsraum und Chief Information Security Officer der Bundeswehr (CISOBw); Professor Dr. Peter Martini, Institutsleiter des Fraunhofer-Instituts für Kommunikation, Informationsverarbeitung und Ergonomie (FKIE); M.A. Merle Maigre, Director NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estland; Herr Iddo Moed, Cyber-Sicherheits-Koordinator im Israelischen Außenministerium; Moderation: Generalleutnant a.D. Dipl.-Inform. Kurt Herrmann, Präsident der Clausewitz-Gesellschaft e.V.) beleuchtete das Thema „Welche Rolle werden künftig passive und aktive Cyber-Verteidigungsfähigkeiten als integrierte Anteile von Operationen in der Militärstrategie einnehmen?“ aus deutscher, israelischer und NATO-Sicht. Dabei wurden die hohe Bedeutung umfassender zivil-militärischer Kooperation für eine wirksame Cyber-Verteidigung unterstrichen, der Cyber- und Informationsraum als fünfte operative Domäne neben Land, Luft, See und Weltraum betrachtet und Cyber-Verteidigung als ein integraler Bestandteil der kollektiven Verteidigung der NATO herausgestellt. Breite Übereinstimmung bestand u.a. in der Auffassung, dass zuverlässige „Attribution“ von Angreifern, ein jeweils umfassendes Lagebild und hinreichende Kooperation im nationalen sowie auch im Bündnis- oder Koalitionsrahmen unverzichtbare Voraussetzungen für eine wirksame Cyber-Verteidigung sind, Cyber-Verteidigung eine gesamtstaatliche Aufgabe darstellt und angestrebte Cyber-Abschreckungsfähigkeiten glaubwürdig sein müssen.

Das Panel 3 ging der Frage „Wie sollten künftige Militärstrategien den sich dynamisch ändernden Herausforderungen im Cyber- und Informationsraum im Rahmen hybrider Kriegsführung begegnen?“ nach. Das Panel bestand aus Dr. Florian Schaurer und Fregattenkapitän Dr. Patrick Jungkunz, beide Referenten im Bundesministerium der Verteidigung, Major i.G. Dipl.-Ing. (FH) Christian Arendt von der NATO CIS Group bei SHAPE sowie dem Moderator, Dr. Martin C. Wolff, Mitglied des Clausewitz-Netzwerkes für Strategische Studien (CNSS). Die Referenten stützten sich auf eine Definition der hybriden Kriegsführung ab, der eine flexible Mischform von

offen und verdeckt zur Anwendung gebrachten regulären und irregulären, symmetrischen und asymmetrischen, militärischen und nicht-militärischen Konfliktmitteln zugrunde liegt. Die Kräfte und Mittel werden mit dem Zweck zum Einsatz gebracht, die Schwelle zwischen den insbesondere völkerrechtlich so angelegten binären Zuständen Krieg und Frieden zu verwischen. Im Verlauf der Paneldiskussion sowie auch bei der erweiterten Diskussion mit dem Auditorium wurde insbesondere die Notwendigkeit einer Strategie für gesamtstaatliche Verteidigung hervorgehoben und dabei eine künftig noch stärkere Ausrichtung auf intensive zivil-militärische Verteidigung gefordert. Da nach Auffassung der Panellisten 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. 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.

Das Panel 4 (Professor Dr. Götz Neuneck, Stellvertretender Wissenschaftlicher Direktor am Institut für Friedensforschung und Sicherheitspolitik, Universität Hamburg (IFSH); Botschafter a.D. Michael Biontino, ehemaliger Ständiger Vertreter der Bundesrepublik Deutschland bei der Abrüstungskonferenz in Genf; Ministerialrat Dr. Ernst-Christoph Meier, Bundesministerium der Verteidigung, Referatsleiter POL II 5; Moderation: Brigadegeneral a.D. Dipl.-Psych. und Dipl.-Pol. Helmut Ganser, Berater für multilaterale Sicherheitspolitik) analysierte „Chancen und Möglichkeiten von Maßnahmen zur Vertrauensbildung, Rüstungskontrolle und Abrüstung hinsichtlich militärischer Fähigkeiten in Verbindung mit künstlicher Intelligenz und Autonomen Waffensystemen“. Einleitend kam die derzeit krisenhafte Lage von Rüstungskontrolle zur Sprache. Das Panel griff dann zwei Schwerpunkt auf: Waffensysteme mit autonomen Fähigkeiten und Anwendung Künstlicher Intelligenz in Planungs- und Führungsprozessen. Neben einem umfassenden Überblick zum aktuellen Stand der Gespräche der „Group of Governmental Experts (GGE) on Lethal Autonomous Weapons (LAWS)“ wurden sowohl die definitorischen Probleme als auch die sehr unterschiedlichen Haltungen von Staaten in Genf zu Rüstungskontroll-Regelungen verdeutlicht. Behandelt wurden ebenfalls KI als „Dual-use Technologie“ und die Komplexität von Systemen mit autonomen Fähigkeiten. Der Fokus richtete sich dann auf sechs Felder sicherheitspolitischer Implikationen von KI und Systemen mit autonomen Fähigkeiten sowie auf Rüstungskontroll-Aspekte. Breiten Raum nahmen dabei die Chancen und Möglichkeiten zur Definition, Implementierung und Verifikation von Verhaltensregeln für Rüstungskontrolle bezüglich KI und Waffensystemen mit autonomen Fähigkeiten ein.

Das Panel 5 stand unter dem Thema „Ist ein sicherheitspolitischer Paradigmenwechsel angesichts der zu erwartenden neuen militärischen Fähigkeiten und Strategien erforderlich?“. Unter der Moderation von Brigadegeneral a.D. Dipl.-Ing. Hans-Herbert Schulz, Geschäftsführer der Clausewitz-Gesellschaft e.V., diskutierten MdB Dipl.-Inform. Alexander Müller, FDP, Mitglied

im Verteidigungsausschuss des Deutschen Bundestages; Generalleutnant a.D. Friedrich-Wilhelm Ploeger, ehemaliger Stellvertretender Befehlshaber Allied Air Command, Ramstein; Frau Sabine Gilleßen, Politikberaterin und Dr. Olaf Theiler, Referatsleiter „Zukunftsanalyse“ im Planungsamt der Bundeswehr. Betrachtet wurden zunächst wesentliche relevante Aspekte der Digitalisierung und die Forderung nach einer verstärkten Ausrichtung aller Bereiche auf prozessorientierte Strukturen sowie signifikant verbesserte Sicherheit und Benutzerfreundlichkeit. Verdeutlicht wurde die Notwendigkeit zu rascher und nachhaltiger Stärkung der Sicherheit und nationalen Verteidigungsfähigkeiten im Cyber- und Informationsraum, verbunden mit der Forderung nach den notwendigen Investitionen und einem dreifachen Paradigmenwechsel. Hinsichtlich der künftigen militärischen Fähigkeiten und Strategien wurde für eine weiterhin konsequente Beachtung und Umsetzung der sicherheitspolitischen Vorgaben, vor allem unter Beachtung des multinationalen Rahmens und der umfassenden Vernetzung, plädiert. Bestimmt wurde die Diskussion zum Einsatz von Waffensystemen mit KI und autonomen Fähigkeiten ebenfalls von Begriffen wie Prävention, Resilienz, Führungsfähigkeit und völkerrechtskonformen Verhaltens- sowie Einsatzregeln. Das Panel gelangte zu der Auffassung, dass alles daran gesetzt werden müsse, zu der Sicherheitsarchitektur zurückzukehren, die bis vor einigen Jahren galt, wozu gesicherte Verteidigungsfähigkeit, Dialogbereitschaft und vertrauensbildende Maßnahmen gehörten. Hinzukommen müsse eine Stärkung der Resilienz der Gesellschaft und eine deutliche (Wieder-)Aufwertung der Gesamtverteidigung. Zudem solle alles darangesetzt werden, zu Verhaltensmaßregeln („Code of Conduct“) zu kommen und diese in ein internationales Rechtssystem einzubinden, für das es idealerweise auch ein Kontroll- und Verifikationsregime geben müsse.

Mit Veröffentlichung des vorliegenden Sammelbandes verbindet die Clausewitz-Gesellschaft die Hoffnung und Erwartung, hilfreiche Gedankenanstöße für den notwendigen Diskurs über die Auswirkungen und notwendigen Konsequenzen moderner Technologie auf die künftige Sicherheitspolitik und Strategie liefern zu können.

Clausewitz hat vor 200 Jahren nicht nur auf die Bedeutung des Zusammenspiels von Politik und Militär für die Sicherheit, sondern auch auf den „Chamäleon-artigen Charakter“ von Konflikten und Kriegen und auf das komplexe Verhältnis sowie die damit verbundene dynamische Interaktion von Politik, Militär und Bevölkerung hingewiesen.

Vor dem Hintergrund der ungeheuren Veränderungen durch moderne Technologien, die alle Lebensbereiche durchdringen und traditionelle Grenzen unterschiedlichster Art auflösen, bedarf es heute – wahrscheinlich mehr als je zuvor - einer frühzeitigen und nachhaltigen Befassung mit den Auswirkungen dieser Technologien und einer ganzheitlichen strategischen Vorausschau im Rahmen eines umfassend vernetzten Sicherheitsansatzes. Seitens der Clausewitz-Gesellschaft wollen wir diesen Diskurs nach besten Kräften fördern und begleiten.

Wolfgang Fett und Werner Baach haben mit feinem Gespür, großem Einsatz und bewundernswerter Akribie dem Sammelband Form und Inhalt verliehen. Mein Dank und der Dank aller Mitglieder der Clausewitz-Gesellschaft e.V. geht an beide und an alle Autoren, Referenten und Moderatoren für ihre wertvollen und interessanten Beiträge, die sie uns kostenlos zur Verfügung gestellt haben.

Allen Lesern wünsche ich, dass sie die in unserem Sammelband vorgenommene Zusammenstellung ansprechend finden und bei der Durchsicht des Kompendiums auf zahlreiche Beiträge stoßen, die ihr Interesse wecken und dadurch ggf. auch den erwünschten sicherheitspolitischen Diskurs beleben. Dialogbereitschaft und konstruktiv kritische Begleitung, z.B. durch Rückäußerungen mit Anregungen oder auch weitergehende Nachfragen, sind stets willkommen.

In diesem Sinne wünsche ich Ihnen viel Freude sowie inhaltliche Anregungen und geistigen Gewinn beim Lesen!

Ihr

Generalleutnant a.D. Dipl.-Inform. Kurt Herrmann

Präsident der Clausewitz-Gesellschaft e.V.