Panel 5:

„Ist ein sicherheitspolitischer Paradigmenwechsel angesichts der zu erwartenden neuen militärischen Fähigkeiten und Strategien erforderlich?“

Einführung des Moderators Brigadegeneral a.D. Hans-Herbert Schulz

Unser Thema fragt nach der Notwendigkeit eines sicherheitspolitischen Paradigmenwechsels und gibt Gelegenheit, die bisherigen Ergebnisse und Erkenntnisse der Tagung einfließen zu lassen. Schauen wir also, ob es uns gelingt, sozusagen eine „Schlussapotheose“ hinzubekommen.

Wie wir sehen werden, kann man die Fragestellung durchaus sehr unterschiedlich verstehen, verschiedene Formen eines sicherheitspolitischen Paradigmenwechsels sind denkbar, je nachdem wie weit oder eng „Sicherheitspolitik“ verstanden wird. (und ob der Schwerpunkt auf politische, militär- bzw. sicherheitspolitische, oder militärische Aspekte gelegt wird).

Und schließlich darf auch die Frage gestellt werden, ob überhaupt noch akzeptierte Paradigmen existieren, in einer „Welt, die aus den Fugen geraten ist“, um ein inzwischen geflügeltes Wort unseres damaligen Außenministers und heutigen Bundespräsidenten zu zitieren. Spätestens seit 2014 sind viele der bis dahin geltenden Grundüberzeugungen ins Wanken gekommen, hinzu kommt ein amerikanischer Präsident, der sich offenbar als „Dekonstrukteur“ der internationalen Ordnung versteht.

Sabine Gilleßen, Politikberaterin:
Meine Aufgabe ist, glaube ich, tatsächlich mehr über den Paradigmenwechsel und die Auswirkungen auf die Sicherheitspolitik zu sprechen. Das ist etwas, was in den letzten zwei Tagen ein bisschen kurz gekommen ist. Letztendlich besteht die Digitalisierung zu 20 % aus Technik und zu 80 % aus Kommunikation, Organisation und Prozess.
Ich würde ganz gerne sagen, was die drei Bereiche für die Sicherheitspolitik und die Bundeswehr bedeuten, sowohl Kommunikation, Prozess als auch die Organisation.

Ich fange mit der Organisation an. Wenn wir über Digitalisierung sprechen, und das heißt natürlich KI, das heißt aber auch, alle anderen digitalen Themen, die dahinterstecken. Digitales Denken und Arbeiten ist ein sehr agiles Arbeiten in Netzen.

Die Bundeswehr ist eine nicht ganz so agile Einheit, zumindest von der Struktur her eine sehr klassische Linienorganisation. Das trifft übrigens auch auf jeden Daxkonzern und alle anderen zu. Aber die Struktur eines Militärs ist immer logischerweise eine sehr viel hierarchischere.

Daher kann man sich schon überlegen, warum das mit der Digitalisierung in hierarchischen Organisationen ein bisschen schwieriger ist. Das heißt auch, dass die Organisation auf den Prüfstand gestellt wird. In Netzen sind die Strukturen nicht so klar, zumindest sehen sie chaotischer aus. Das müssen sie nicht zwingend sein. Aber in Netzen arbeitet es sich einfach komplett anders. Prozesse müssen anders organisiert werden. Das ist auch Digitalisierung,

dafür zu sorgen, dass man tatsächlich digital arbeiten kann. Das ist der Prozess. Das ist ganz, ganz wesentlich, denn wie will man konkurrieren oder mithalten mit anderen Armeen oder mit anderen Einheiten, die da einfach viel besser aufgestellt sind? Insofern ist der Prozess ganz wichtig.

Zum Prozess gehört aber auch die Sicherheit. Die Frage zum Beispiel ist leider gar nicht aufgekommen, was eine gute Sicherheitstechnologie sein könnte, um bestimmte Dinge abzusichern. Eine wichtige Frage ist auch, ob alle die Folgen einschätzen können, wenn sie solche Messenger wie WhatsApp einsetzen? Das Problem ist immer, dass man eine Balance herstellen muss zwischen der Sicherheit, die einen Verlust an Benutzerfreundlichkeit beinhaltet, und der Benutzerfreundlichkeit, die wir brauchen, damit ein Verfahren überhaupt akzeptiert wird. Es gibt keine hundertprozentige Sicherheit – weder digital noch analog.

Da gibt es ganz neue Herausforderungen in punkto Sicherheit angeht, und man muss einfach akzeptieren – auch ein Paradigmenwechsel – dass nichts mehr geheim bleibt.

Und meine These wäre jetzt zu sagen, dass wahrscheinlich 99 % dessen, was im Moment geheim gehalten wird oder als geheim zu halten eingestuft wird, man auch veröffentlichen könnte, ohne dass die Welt deswegen untergeht. Ich glaube, der Paradigmenwechsel besteht darin, dass man sich tatsächlich noch einmal überlegt, was man eigentlich wirklich geheim halten muss und was nicht. Weil, und das ist der dritte Bereich, die Kommunikation, heutzutage in digitalen Zeiten eine ganz andere ist. Information steht zur Verfügung. Permanent. Wir haben genug Beispiele dafür. Es ist nicht nur Snowden und Wikileaks und was weiß ich. Es gibt genug Beispiele dafür, dass auch Informationen, die früher niemals öffentlich geworden wären, auf einmal öffentlich geworden sind.

Die durchaus weit verbreitete Taktik, Informationen nicht rauszugeben, das funktioniert nicht mehr. Das ist ein wesentlicher Paradigmenwechsel. Und das hat gar nicht so viel damit zu tun, ob man KI einsetzt oder wie auch immer, sondern das sind einfach die geänderten Rahmenbedingungen, in denen die Bundeswehr agieren muss. Und wenn wir, wie gestern, über Frage von externem Einfluss auf soziale Medien reden und ähnlichem mehr, dann ist es auch notwendig, dort zu kommunizieren. Die Bundeswehr ist ja auf diesen Plattformen auch aktiv. Aber jeder einzelne Soldat, jede einzelne Soldatin sind auch immer Repräsentanten der Bundeswehr. Und das muss goutiert werden. Das ist auch ein Paradigmenwechsel.

Auch zu Kommunikation uns Sicherheit noch einen Hinweis: Es geht tatsächlich auch darum, Angriffe auf die Demokratie zu verteidigen. D.h. aber, dass wir auch zu einer ganz neuen Debatte kommen müssen, welche Aufgabe kann die Bundeswehr haben, wenn also nicht Menschen, Gebäude, Landesteile angegriffen, sondern Demokratie über soziale Medien? Es gibt keine Blaupause für so eine Debatte und auch tatsächlich keine abschließenden Antworten.

Ich sage mal so eine ganz falsche Antwort ist dann so eine Sache wie Schwarztrojaner oder dergleichen zu beschließen, weil das letztendlich nur zu neuen sicherheitspolitischen Lücken führt. Ich weiß nicht, ob Sie das Konzept kennen. Da hat die Bundesregierung beschlossen,

dass man Softwarehersteller auffordert, Sicherheitslücken zu lassen, damit der BND, Verfassungsschutz oder wer auch immer, sich in Geräte einhacken kann. Das ist ungefähr genauso klug, wie wenn Sie Ihr gesamtes Haus mit einer tollen Sicherheitstechnik ausstatten, aber die Hintertür nur mit so einem Riegel von außen verschließen. In dem Moment ist die Technik schlicht unsicher, unabhängig von der Frage, ob das mit einer liberalen Republik und Menschenrechten und Informationsfreiheitsrechten und dergleichen kompatibel ist. Das ist eine ganz andere Debatte.

Schön fand ich, dass hier immer wieder gesagt worden ist, dass wir die ethische Debatte führen müssen. Ich bin Mitglied in zwei Ethikräten: Digitalisierung und Ethik und KI und Ethik. Das Justizministerium hat in dieser Woche die Datenethikkommission eingerichtet. KI ist genau das, was wir programmieren. Die KI macht das, was wir vorher sagen. Und wir können einen gewissen Pragmatismus hinein programmieren, aber das ist es dann auch.

Deshalb ist so eine Ethikdebatte ganz wichtig. Und deshalb kann man auch nicht sagen, automatisierte Systeme sind objektiv, wie es so oft suggeriert wird.

Der Paradigmenwechsel ist riesig. Die Debatten, die Fragestellungen, die sich daraus ergeben, jetzt unabhängig von technischen Debatten, aber die Fragestellung gerade zur Sicherheitspolitik für die innere und äußere Organisation der Bundeswehr, finde ich, sind enorm. Aber sie sind auch ganz spannend, weil ich glaube, dass es noch einmal viele Möglichkeiten schafft. Und deshalb finde ich auch diese Denkfabrik super, die bringt letztendlich auch die unterschiedlichen Ebenen zusammen, weil auch das Digitalisierung ist, dass die Hierarchie ein bisschen aufgelöst wird, was in der Bundeswehr zuweilen kritisch ist. Aber genau um solche Ansätze geht es und darum, das Wissen, das da ist, unabhängig vom Dienstgrad, konstruktiv einzubringen. Und deshalb freue ich mich auch, dass ich heute eingeladen bin als Zivilistin, die immer mal wieder über das eine oder andere lächelt, wie sie wahrscheinlich auch über das eine oder andere lächeln, wenn ich etwas sage. Aber das finde ich, das macht viel Spaß und ich freue mich auf die Debatten.

Alexander Müller, MdB (FDP):
Kommen wir zum Thema, zu der Frage nach dem sicherheitspolitischen Paradigmenwechsel. Ich darf mit einem Zitat, einem bemerkenswerten Zitat unserer Einladung, beginnen, der zweite Satz aus der Einladung ist: „Die Wahl der geeigneten Mittel sowie des rechten Maßes der Mittel für die Gewaltanwendung, um einen Gegner zur Erfüllung unseres Willens zu zwingen.“ Das klingt nach Clausewitz als Kern einer Strategie die Möglichkeiten des Handelns, also des rechten Maßes der Mittel für die Gewaltanwendung. Das finde ich einen ganz bemerkenswerten Satz angesichts der Möglichkeiten, die wir heute haben.

Stuxnet war ein Virus, der 2010 sehr weite Verbreitung gefunden hat. Er hat sich sehr weit verbreitet und hat erst einmal sehr wenig gemacht. Auf Windows-Systemen hat er eigentlich nur für seine eigene Verbreitung gesorgt. Und dann ist der Virus hingegangen, sobald er gemerkt hat, er ist an einem Siemens-System, an einer Prozesssteuerung, das System zu manipulieren. Und dieser Virus hat es geschafft im Iran Zentrifugen, Uranzentrifugen, die

notwendig sind, um Uran hoch anzureichern, um waffenfähiges Material zu erzeugen, zu zerstören, indem er die Drehzahl manipuliert hat, und zwar so manipuliert hat, dass die Dinger kaputt gegangen sind.

Gezielte Wirkung, unblutig, keine Kinetik, überhaupt keine Kinetik eingesetzt, Attribution des Verursachers verschleiert. Es weiß bis heute keiner genau, wer steckte dahinter. Also es ist im Grunde die perfekte Waffe im 21. Jahrhundert.

Man vermutet, dass das eine Israelisch-US-Kooperation war, man vermutet, dass das Team mindestens fünf bis zehn Programmierer umfasst haben muss, weil das eine sehr schwierige Operation war, aber es zeigt heutige Möglichkeiten. Für mich ist das das klassische Beispiel einer Waffe, die perfekt ist, die genau im Clausewitzschen Sinne ein Mittel der Anwendung von Gewalt zu ihrem Willen. Sie haben ihren Willen erreicht, sie haben das iranische Atomprogramm zerstört und haben es unblutig gemacht. Das ist so das klassische Beispiel.

Wo wir beim Iran sind, da gibt es andere Beispiele: Am 4. September 2011 hat der Iran es geschafft, eine CIA-Drohne vom Himmel zu holen. Auch das nicht kinetisch. Der Iran selber sagt, man hätte die Funksignale, die Steuersignale zu der Drohne manipuliert und man hätte zum gleichen Zeitpunkt die GPS-Signale gehackt, also falsche GPS-Signale gesendet. Fakt ist, dass Ding ist sauber gelandet, also ohne kaputt zu gehen. Es gab eine kleine Beschädigung an der Tragfläche. Aber die Iraner haben das Ding sauber gelandet und haben es im Anschluss exakt analysiert.
Merke: Die Übernahme eines feindlichen Waffensystems mit Cyber-Mitteln ist möglich. Nun sind die Iraner nicht bekannt als die Speerspitze des weltweiten IT-Wissens. Also auch das sollte uns allen im Hinterkopf bleiben, was das für ungeahnte Möglichkeiten hat. Nicht nur ein feindliches Waffensystem komplett zu übernehmen, sondern es möglicherweise gegen den Feind selber zu richten. D.h., sie schaffen es vielleicht, dass die Artillerie das Geschütz um 180 Grad dreht und schießt. Das sind alles Dinge, die sollte man im Jahr 2018 in Erwägung ziehen.

Ein weiteres kleines Beispiel, was möglich ist: Am 23. Dezember 2015 ist ein Angriff auf die ukrainische Stromversorgung erfolgt. Man weiß auch nicht, wer es war, man kann es sich aber denken. Die Netzwerktechnik ist damals angegriffen worden. Es gab einen dreistündigen Stromausfall. Dass es nur drei Stunden waren, ist glimpflich.

Jetzt überlegen Sie sich das mal wir, in Mitteleuropa, in Deutschland, wir hätten einen mehrstündigen größeren Stromausfall, was das bedeutet für unsere Zivilisation? Ja, das ist nicht nur der Kühlschrank, die Gefriertruhe, die dann plötzlich auftaut, das ist ärgerlich. Das fängt an mit Krankenhäusern. Glauben Sie nicht, dass alle Krankenhäuser in Deutschland eine funktionierende Notstromversorgung haben, die das ganze Spektrum abdecken kann. Wir testen es ab und zu. Meistens funktioniert es auch. Aber es ist nicht gesichert, dass das alles funktioniert. Nehmen Sie Rechencenter zum Internet. Da sind die wenigsten mit Notstromversorgung gesichert. Dann geht das weiter mit Tankstellen. In dem Moment, in dem kein Strom mehr da ist, wird keine Tankstelle mehr eine Pumpe haben, an der Sie Ihre Autos betanken können. Supermärkte: die Kassen funktionieren nicht mehr. Die Deutsche

Bahn fährt mit Strom. Sie können innerhalb einiger Stunden die komplette Infrastruktur in Deutschland lahmlegen, wenn Sie das Stromnetz angreifen.

Und da muss man dann die Rechtslage kennen. Ich muss mit meinem Moped alle zwei Jahre zum TÜV. Das wird auf Herz und Nieren überprüft, und mein Auto auch, um die Gefahr, die von diesen Geräten ausgeht, zu kontrollieren. Aber ein Betreiber eines Kohlekraftwerks oder ein Netzbetreiber darf das rein freiwillig analysieren, ob seine Netze sicher sind oder nicht. Da kommt ab und zu einer vom BSI vorbei und schaut mal, gibt Ratschläge. Aber ob das umgesetzt wird, das ist dann den Betreibern überlassen. Das ist die Rechtslage in Deutschland.

Dann überlegen Sie, was man da alles angreifen könnte: Wasserversorgung, Gasversorgung, Banken, Zahlungsverkehr könnte man lahmlegen, Verkehrsinfrastruktur, ich habe es genannt, die Bahn. Da sind sehr viele Angriffsvektoren, die ein potentieller Feind angreifen könnte.

Eine kleine Frage an die Runde, damit Sie alle wach werden, wer von Ihnen hat denn heute kein Mobiltelefon am Mann? Das sind zwei Hände voll, also überschaubar. Wer von Ihnen, der ein Mobiltelefon dabei hat, hat denn dauerhaft die GPS-Funktion gesperrt? Ah ja, das ist doch ein Drittel des Saales würde ich sagen. Jeder, der sich jetzt nicht gemeldet hat, muss wissen, dass von ihm Bewegungsprofile bei irgendeinem Provider hinterlegt sind. Entweder bei Apple oder bei Google oder sonst sonst wem. D.h. ein Provider hat von Ihnen das Bewegungsprofil. Er weiß, wie Sie sich bewegen. Der hat die Daten, mit wem Sie sich treffen. Der weiß also, welche anderen Telefone hier noch vorhanden sind und dass Sie heute auf einer militärischen Tagung sind. Der weiß eine ganze Menge über Sie und kann diese Dinge miteinander verknüpfen. Ob sie es machen, in welchem Maße sie es machen, sei mal dahingestellt. Aber es gibt diese Daten. Dessen muss sich einfach jeder bewusst sein. Das hat ja auch die Kollegin Gilleßen eben auch schon angesprochen.

Und dann kommen wir zu den Fähigkeiten Deutschlands. Was kann denn Deutschland in diesem Gebiet im Bereich Cyber-Verteidigung, Cyber-Angriffe? Ich selber habe in diesem Jahr jetzt insgesamt vier Wochen Reserveübungen gemacht, davon drei Wochen im Kommando Cyber- und Informationsraum. Ich denke, ich kenne den Laden mittlerweile einigermaßen. Ich bin dort auch von Dezernat zu Dezernat, von Abteilung zu Abteilung gegangen und habe mir mal unsere Fähigkeiten angeguckt und bin zum Teil beeindruckt von den Fähigkeiten, die wir haben. Wir haben sehr gute Soldaten, sehr motivierte und wirklich gute Fachleute. Die Zahl ist allerdings ausbaufähig, würde ich mal sagen. Ich muss jetzt ein bisschen vorsichtig sein, weil ich Geheimnisträger bin und musste da etliche Papiere unterschreiben, dass ich davon nichts verrate. D.h. Sie werden von mir keine Zahlen und nichts Genaues hören. Und der nächste Satz wird ein bisschen gestelzt klingen, ich darf nämlich nur erzählen, was sowieso öffentlich bekannt ist. Aber Spiegel Online schrieb im Herbst 2015 von einem Angriff auf ein afghanisches Mobilfunknetz, und zwar in Spiegel Online vom 23.9.2016, dass angeblich in Afghanistan eine Entwicklungshelferin von der GIZ entführt worden ist. Es gab einen Krisenstab der versucht hat, die Dame zu befreien. Und dieser Krisenstab hätte angeblich eine Einheit, Computer Network Operations, CNO aus Rheinbach, damit beauftragt, das Handynetz zu hacken und das hätten die angeblich auch

gemacht und hätten die Mobiltelefone der Entführer lokalisieren können, so dass der Krisenstab dann wusste, wo die sich aufhalten. Damit in den Lösegeldverhandlungen man sich auch sicher sein konnte, dass die tatsächlich noch mit ihrer Geisel dort sind.
Das stand in Spiegel Online, und es ist auch von der Bundesregierung nicht dementiert worden. Mehr darf ich dazu nicht sagen. Aber das gibt Ihnen einen Eindruck, wie die Fähigkeiten sind.

Ich fasse es zusammen: Es gibt enorme Möglichkeiten, die man heute mit Cyber-Angriffen durchführen kann. Ich glaube, ich habe Ihnen das ein bisschen dargestellt. Es ist enorm wichtig, dass wir Cyber-Verteidigungsfähigkeiten auch aufbauen. Das ist auch enorm wichtig. Ich glaube, das erklärt sich aus meinem Vortrag von selbst.

Die militärischen Operationen werden heute anders geführt als es früher der Fall war, mit anderen Mitteln. Mein Gefühl ist auch, jetzt kommen wir zum Thema Paradigmenwechsel, dass die Bundeswehr teilweise noch so aufgestellt ist, als würden militärische Auseinandersetzungen heute so geführt wie vor 30, 40 Jahren. Wir müssen da ein Stück weit deutlich stärker in die Cyber-Fähigkeiten investieren. Das ist meine feste Überzeugung. Und daher die Antwort auf die Frage, ist ein sicherheitspolitischer Paradigmenwechsel nötig? Ich will nicht sagen, dass wir bis jetzt alles falsch gemacht, aber ich will ein deutliches Ja auf diese Frage sagen mit der Richtung, dass wir mehr in die Cyber-Kapazitäten der Bundeswehr hineininvestieren müssen.

Letzter Satz zu den autonomen Systemen und der künstlichen Intelligenz, diesbezüglich ist die Haltung der FDP genau wie die der Bundesregierung. Wir müssen unbedingt ein internationales Verbot hinbekommen. Daran sollten alle arbeiten. Aber ich denke, die Hoffnung, dass das gelingt ist gering. Es sieht im Moment nicht danach aus, dass das auch erreicht wird. Natürlich müssen die Bemühungen sein, aber wir müssen gewappnet sein, dass irgendjemand diese Dinge entwickelt und wir sollten als Bundesrepublik Deutschland in der Lage sein, uns zu verteidigen gegen diese Systeme. Das ist möglich. Mit Sicherheit. Wenn Sie sich in einen Programmierer eines solchen Systems hineinversetzen, haben Sie mit Sicherheit den Auftrag, dass ein autonomes Systeme, wenn es töten soll, immer ganz sicher sein muss, dass das ein feindlicher Kombattant ist. Wenn da irgendein Zweifel besteht, wird so ein System immer zögern und sich zurückziehen und nicht töten.

Und d.h. auch immer, Sie haben die Möglichkeit so ein System ebenfalls anzugreifen. Es wird mit Sicherheit Codes geben, dieses zu reaktivieren. Gäbe es sie nicht, würde der Entwickler selber mit seinem Leben spielen. Es gibt immer irgendeinen Code, um das Ding zu reaktivieren. Darauf sollten Sie auch Ihre Fähigkeiten trainieren, dass Sie herausfinden, wie Sie so etwas bekämpfen können.

Dr. Olaf Theiler, Referatsleiter Zukunftsanalyse, Planungsamt der Bundeswehr:

Die Entwicklungen der letzten 5 bis 10 Jahre haben eines deutlich gemacht, Krieg ist auch in Europa wieder führbar geworden.
Wir bewegen uns derzeit in der so genannten VUCA-Welt. Sie ist gekennzeichnet durch Begriffe wie *Volatility*, also Unbeständigkeit (die Ausschläge erfolgen nicht nur schneller, sondern fallen auch sehr viel stärker aus), *Uncertainty*, Unsicherheit (die Veränderungen werden von bisher nicht erwarteten Variablen und Kausalbeziehungen getrieben), *Complexity* (die Wechselwirkungen verschiedenster Variablen spielen eine große Rolle und erschweren jegliche Analyse), sowie *Ambiguity*, also eine Viel- oder Mehrdeutigkeit (bei der eindeutige Interpretationen von Informationen, Akteuren und ihren Absichten nicht mehr möglich ist). Vor diesem Hintergrund wird gerade die Sicherheitspolitik zukünftig maßgeblich durch Faktoren wie „Komplexität" und „Wandel" geprägt werden. Von relativ statischen, in ihren Dimensionen klar überschaubaren strategisch-taktischen Herausforderungen zum Ende des Kalten Krieges hat sich schon längst ein Wechsel zu unübersichtlicheren Operationen des Krisenmanagements auf regionaler, später sogar globaler Ebene vollzogen. Dazu kommen inzwischen noch Elemente der "klassischen Kriegführung" im Rahmen der Bündnis- und Landesverteidigung, aber gerade in diesem Zusammenhang auch noch Aspekte asymmetrischer bzw. hybrider Kriegführung hinzu. Da gleichzeitig die Möglichkeit der Einsätze zum Krisenmanagement bestehen geblieben sind, mit all ihren Herausforderungen, steigert das die Unübersichtlichkeit möglicher militärischer Anforderungen und Herausforderungen noch einmal deutlich.
Nimmt man dazu noch die ebenso erschreckenden wie simplen Erkenntnisse der Geschichtsforschung, sollte einem das Ausmaß der aktuellen Entwicklungspotentiale deutlich werden. So wurde eine britische Militärhistorikerin vor einer Weile gefragt, warum es Kriege gebe. Ihre Antwort war einfach: Weil es Menschen gibt, die glauben sie gewinnen zu können". Diese Lektion gilt es auch in Deutschland wieder als allgemeingültig zu akzeptieren, gerade wenn wir einen Krieg in Zukunft verhindern wollen. Denn obwohl wir in der Nachkriegszeit seit 1945 im Grunde in einem politischen und völkerrechtlichen System leben, dessen Zweck es u.a. war, Kriege durch Regulierung so unnötig und unmöglich wie nur möglich zu machen, muss man doch akzeptieren, dass dies wahrscheinlich nicht dauerhaft von Erfolg sein kann. Denn am Ende sind Kriege und Konflikte Elemente unserer Geschichte, der Drang zum gewaltsamen Austragen fundamentaler Konflikte deutlich älter als alle Errungenschaften der Zivilisation. Wenn es stimmt, dass „War, like a virus, must mutate to survive"[1], dann müssen wir – trotz aller Friedensbemühungen und aller Hoffnungen auf den Gedanken des Rechts und der Völkergemeinschaft – uns mit der Sorge auseinandersetzen, dass man Krieg nicht nur durch Regulierungen vermeiden können wird.
Eine weitere Folge der neuen Unübersichtlichkeit ist es, dass man nicht mehr auf eine klare, wahrscheinliche Bedrohung hin planen kann. Stattdessen wiegen die unterschiedlichen Möglichkeiten von krisenhaften Entwicklungen schwerer, auf die man sich nicht gleichwertig vorbereiten kann. Der Weg der Wahrscheinlichkeiten lässt jedoch zu viele eventuell verhängnisvolle Möglichkeiten außer Acht, ein Ansatz, den man sich in Zeiten hoher Volatilität nicht mehr leisten kann. Im Ergebnis muss man neue, flexible, anpassungsfähige

[1] Siehe dazu David Patrikarakos: War in 140 Characters: How Social Media is Reshaping Conflict in the Twenty-First Century.New York 2017, S.6 ff.

und vor allem schnellere Wege der Fähigkeits- und Rüstungsplanung und Beschaffung entwickeln. Die Anfänge dazu sind in der Bundeswehr bereits gemacht, jetzt gilt es diesen Weg konsequent weiter zu gehen.
Mit Klein, Flexibel, Adaptiv und Schnell sind auch die neuen Herausforderungen auf dem Gefechtsfeld beschrieben. Die Rückkehr der Masse auf das Gefechtsfeld z.B. in Form von Schwarmangriffen, überfordert aktuelle Abwehrsysteme. Dadurch steigt u.a. auch die Notwendigkeit zur Digitalisierung, die mehr Transparenz und schnelleres Handeln im Gefecht bringen soll. Die logische Folge sind dann Systeme, mit denen der Akteur vor Ort das gleiche Informationsniveau wie das rückwärtige HQ bekommt. Nur das wir uns schon aus Zeitgründen nicht mehr leisten können, Informationen erst im HQ auszuwerten, bevor vor Ort gehandelt werden kann. Zentralisierte Führung wird damit nicht nur unnötig, sie wird ein Problem. Denn gerade die Digitalisierung wird verführerische neue Optionen für das Mikromanagement schaffen, die neue Transparenz einen zusätzlichen Druck zur strategischen Kontrolle, während gleichzeitig die Handlungsgeschwindigkeit vor Ort konsequent zunimmt und immer weniger Spielraum für zeitaufwendiges Abwägen und Reflektieren lässt. Unter diesen Bedingungen wird der hoch ausgebildete Gefechtsoffizier als Gegengewicht zum ebenso befähigten Stabsoffizier eine Notwendigkeit. Ihm werden im Sinne der Auftragserfüllung neue Formen der direkten Führungsunterstützung in Form von digitalen Systeme (Sensoren ebenso wie Datenverarbeitung) zur Verfügung gestellt werden müssen, insbesondere in Form von Entscheidungsunterstützung durch künstliche Intelligenz. Am Ende wird die Überlebensfähigkeit im Gefecht die unmittelbare Bearbeitung einer enormen digitalen Informationsflut vor Ort erfordern. Dafür gilt es ein neues Geleichgewicht zwischen zentraler (strategischer) Steuerung und dezentraler (taktischer) auftragsorientierter Handlungsfreiheit gefunden werden müssen.

Folien gesondert übermittelt

Generalleutnant a.D. Friedrich Wilhelm Ploeger:

Ausgehend von der Zielsetzung, dass jede Bundesregierung Recht und Freiheit des deutschen Volkes in Sicherheit gewährleisten will, möchte ich zunächst analysieren,

welche grundlegenden Muster und Denkweisen („Paradigmen“) das sicherheitspolitische Handeln bestimmen. Die wesentlichen Paradigmen sind:

- Die Multilateralität in der Sicherheitspolitik. Weil von der Verfassung vorgegeben, organisiert DEU seine Sicherheit im Bündnis von NATO, EU (in einem „kollektiven Sicherheitssystem“); für Einsätze jenseits der Landesgrenzen ist dies zwingend vorgegeben. Daraus folgt der Grundsatz der Multilateralität in der deutschen Sicherheitspolitik („keine Alleingänge“). Für DEU bildet die VN-Charta als umfassendes Regelwerk den Rahmen, in dem militärische Gewalt legal/ legitim angewendet werden kann; diverse Abkommen regeln bestimmte Waffenarten und Technologien: Nuklearabkommen, NPT, MTCR, B/CWC etc.
- Aus der jahrzehntelang gewachsenen Einbindung in Bündnisse und vor dem Hintergrund der Geschichte resultiert auch DEU Widerwillen, eine Führungsrolle in der Sicherheitspolitik und in sicherheitspolitischen Fragestellungen zu übernehmen.
- Der vernetzte Ansatz, da DEU seine Sicherheit in heutiger Zeit nicht eindimensional national gewährleisten kann. Insbesondere in den Auslandseinsätzen wird geradezu exemplarisch vernetzt gehandelt, im Inland überwiegt leider häufig das Ressortdenken.
- Der Stellenwert von „Äußerer Sicherheit“ und „Verteidigung“ ist am jeweiligen Haushaltsansatz abzulesen. Seit Ende des „Kalten Krieges“ hat DEU hier die Substanz der Streitkräfte aufgezehrt und nur das Notwendigste investiert, um sich an gemeinsamen Kriseninterventionen beteiligen zu können, aber nicht seiner außen- und sicherheitspolitischen Interessenlage und seinem Gewicht in der Welt entsprechend.

Was hat sich nun geändert? Seit der Krim-Annexion 2014 ist Landes- und Bündnisverteidigung wieder mindestens gleichwertig im Verhältnis zu „Krisenbewältigung“. Die europäischen NATO-Partner haben sich verpflichtet, mehr in Verteidigung zu investieren und bis spätestens 2025 gemeinsam vereinbarte Ziele zu erreichen: VgAusgaben entspr. 2%-BIP, darin 20% Investitionen, die Realisierung der „4x30“ Initiative (30 Kampfbataillone, 30 Staffeln Kampfflugzeuge, 30 Großkampfschiffe, einschließlich zugehöriger Logistik!, einsetzbar in 30 Tagen; DEU-Anteil: ca. 10%). Für die Bundeswehrplanung folgte daraus ein dramatischer Paradigmenwechsel. „Trendwenden“ wurden angekündigt, die bislang jedoch ohne überzeugendes Ergebnis blieben; eklatante Schwächen in Verfügbarkeit, Bevorratung, personeller und materieller Durchhaltefähigkeit sind nach wie vor sichtbar.

USA-Präsident Trump hat die Beistandsverpflichtung in der NATO immer wieder in Frage gestellt, auch und gerade weil aus Sicht der USA die europäischen Bündnispartner zu wenig in die Verteidigung investieren. Seit dem Gipfel im Juli scheint nun die Herausforderung und Verpflichtung für die Europäer, insbesondere für DEU, klar, den Art 3 des Washingtoner Vertrages ernster zu nehmen und mehr in die Verteidigung zu investieren. EUR muss - auch ohne Unterstützung durch USA - handlungsfähiger werden („Pivot to Europe“). Hieraus erwächst besondere Verantwortung für DEU (für die

„Nahtod-Erfahrung“ beim letzten Gipfel trägt auch DEU Mitverantwortung!). Die Argumentation, DEU könne wegen seiner Geschichte keine Führungsrolle übernehmen, trägt in EUR nicht mehr (vor allem auch, weil DEU in anderen Fragen, z.B. Finanzkrise sehr wohl den Ton angibt!).

Die auf dieser Konferenz diskutierten neuen Technologien im Bereich Cyber und Künstlicher Intelligenz (KI) konfrontieren uns mit vielfältigen neuer Risiken, die von Staaten und/ oder nicht-staatlichen Gruppierungen ausgehen können. Sie haben durchaus disruptives Potential. Möglichkeiten zur „bindenden vertraglichen Einhegung“ sind kurzfristig eher zweifelhaft (Definitionsprobleme, Interessenlagen von Staaten und Industrien → Geist ist aus der Flasche!). KI ist nicht von best. Rohstoffen abhängig - wie Nuklearwaffen oder B/CW – denkbar erscheint vielleicht eine Art „Code of Conduct“, der sich vor allem an Wissenschaft und Industrie richtet. Zweifel an der Wirksamkeit einer solchen Maßnahme aber bleiben (vgl. MTCR).

Cyber ist von Natur aus transnational. Im Informationsraum verschwimmen nationale Grenzen und damit auch die Grenzen zwischen innerer und äußerer Sicherheit. Daraus folgt die Notwendigkeit alle staatlichen Fähigkeiten (z.B. Verteidigung, Sicherheit, Nachrichtendienste, Technologieforschung etc.) zu vernetzen und auch nationale und multinationale Fähigkeiten (EU und NATO) miteinander zu verknüpfen. Weil in der heutigen Zeit auch kritische Infrastrukturen über die nationalen Grenzen hinweg miteinander vernetzt sind, ist multilaterales vernetztes Handeln unumgänglich. National gilt es, sich wieder auf Lagen, in denen Gesamtverteidigung geleistet werden muss, einzustellen und den dafür notwendigen Werkzeugkasten einschl. rechtlicher Grundlagen bereitzustellen. Dazu gehört auch eine geeignete nationale Führungsstruktur. Ein Paradigmenwechsel auch bei der lange vernachlässigten Zivilverteidigung ist unausweichlich. Staatl. Investitionen in die Härtung und Resilienz kritischer Infrastrukturen (aus meiner Sicht durchaus auf 2%-Ziel anrechenbar!) könnten mit verstärkten Weisungs- und Zugriffsrechten im Bedarfsfalle verknüpft werden. Schließlich stellt sich die Frage, ob die Gewichtung der Uniformträgerbereiche in der veränderten Lage noch passend ist. Nachsteuerungen müssen jetzt erfolgen, da strukturelle Anpassungen in der Regel viel Kraft und Zeit brauchen.

Seit der Annexion der Krim ist „Deterrence“ wieder wichtiges Element. „Deterrence“ muss sich, um glaubwürdig zu sein, auf ein breites Spektrum an konventionellem, nuklearen und Cyber-Fähigkeiten abstützen und durch eine glaubwürdige Politik flankiert sein.

Die Abschreckungswirkung beim Gegner basiert auf einem Mix überzeugender defensiver und offensiver Fähigkeiten, auch im Cyberraum. Hier sind neben funktionierender Härtung insbesondere Fähigkeiten zur Enttarnung verdeckter Operationen wichtig. In der NATO stellt sich die Frage, ob die „Extended Nuclear Deterrence“ unter Trump noch glaubwürdig ist und ob die substrategischen Fähigkeiten der NATO einen glaubwürdigen Link zu den strategischen Systemen der USA darstellen. Eine Debatte um die

Modernisierung des substrategischen Beitrages der europäischen Bündnispartner (DCA) und die DEU nukleare ist überfällig!

Fazit: DEU hatte es sich bequem eingerichtet im Bündnis mit einem Beitrag, wie er für Beteiligung an Kriseninterventionen notwendig war, nicht aber seiner Bedeutung entspricht. Im Zweifelsfall füllten die USA notwendige Fähigkeiten auf. Die Änderungen in den Grundparametern von Sicherheit fordern nun erhebliche Anstrengungen, um die Lücke zu schließen zwischen dem, was DEU sicherheitspolitisch für notwendig hält und unterstützt (nicht selten auch das militärische Engagement von Freunden und Partnern) und dem, was DEU und EUR selbst bereit sind für die eigene Sicherheit zu tun und welche Kosten DEU bereit ist dafür zu schultern. Dies ist der eigentliche Paradigmenwechsel. Eine breite und ehrliche Auseinandersetzung zu der Thematik in der Öffentlichkeit steht aus.

Schlussbemerkungen des Moderators:

Die zusätzlichen, neuen Herausforderungen, Cyber, KI und Autonome Waffensysteme, werfen neue, weitreichende Fragen auf. Bisher gibt es erst wenige Versuche, sie in internationales Recht oder eine Sicherheitsordnung einzuhegen, obwohl sie das Potential haben, ähnlich disruptiv wie Nuklearwaffen zu wirken.

Für die Beantwortung der uns im Panel gestellten Frage heißt das m.E., dass alles darangesetzt werden müsste, zu der Sicherheitsarchitektur zurückzukehren, die bis vor einigen Jahren galt, wozu gesicherte
Verteidigungsfähigkeit und Dialog und vertrauensbildende Maßnahmen gehören. Hinzukommen muss eine Stärkung der Resilienz der Gesellschaft und eine Rückkehr zur Gesamtverteidigung. Angesichts der neuen Herausforderungen, die sich in ihrer Dimension und zukünftigen Wirkung erst abzeichnen, sollte alles darangesetzt werden, zu einem „Code of Conduct“ zu kommen und sie vergleichbar den Nuklearwaffen, in ein internationales Rechtssystem einzubinden, für das es idealerweise auch ein Kontroll- bzw. Verifikationsregime geben müsste. Der Erfolg wurde in den Beiträgen gestern bezweifelt, aber Prof. Lauster und Jay Tuck haben zu Recht darauf hingewiesen, dass auch ein langer Weg mit einem ersten Schritt beginnt, den man aber tun muss.

Zum Autor: Brigadegeneral a.D. Hans-Herbert Schulz ist Geschäftsführer der Clausewitz-Gesellschaft e.V.: