Clausewitz-Gesellschaft • Jahrbuch 2019

Clausewitz-Gesellschaft

Jahrbuch 2019

Eine Publikation der
Clausewitz-Gesellschaft e.V.

ISBN: 978-3-9816962-5-7

Inhalt **Seite**

Sicherheitsvorsorge und Resilienz für Politik, Gesellschaft und Streitkräfte im Zeitalter von Globalisierung und Digitalisierung

Thomas Silberhorn

Die Digitalisierung durchdringt sämtliche Lebensbereiche, die globale Vernetzung schreitet rasch voran. Der fundamentale Wandel durch Informations- und Kommunikationstechnologien verändert das gesellschaftliche, wirtschaftliche und politische Miteinander. Wir stehen damit vor einer komplexer und schnelllebiger werdenden Sicherheitslage. Vor diesem Hintergrund gewinnen Sicherheitsvorsorge und Resilienz enorm an Bedeutung.

Für unsere Streitkräfte eröffnet die Digitalisierung neue Fähigkeiten und Chancen, sowohl physisch als auch virtuell. Für die Gefechtsfelder und Einsatzszenarien der Zukunft werden Zeit, Geschwindigkeit und Reaktionsfähigkeit entscheidende Kriterien für erfolgreiche Operationsführung in allen militärischen Dimensionen sein. Digitalisierung ist hier der entscheidende Schlüssel: Sie erhöht die Informations- und Wirkungsüberlegenheit sowie Durchsetzungsfähigkeit der Streitkräfte auf dem digitalisierten Gefechtsfeld.

Parlamentarischer Staatssekretär Thomas Silberhorn

Gleichzeitig gehen mit der Digitalisierung ernstzunehmende Risiken und Herausforderungen einher. Unsere Energie-, Wasser-, Lebensmittel- und Gesundheitsversorgung sind eng mit dem Cyberraum verknüpft. Unsere Kommunikation läuft zunehmend digital ab. Deshalb ist eine sichere und freie Nutzung des Cyber- und Informationsraumes elementar.

Das macht uns als Gesellschaft und als Staat, genauso wie die Wirtschaft und Industrie verwundbar. Das Spektrum der daraus erwachsenden Bedrohungen ist dabei weit gefächert. Es reicht vom Missbrauch persönlicher Daten und Wirtschaftsspionage über Desinformationskampagnen mit dem Ziel politischer Einflussnahme bis zur Schädigung kritischer Infrastrukturen, wie Elektrizitätswerke, und Störung der Regierungskommunikation. Diese Schwachstellen werden nicht nur von Kriminellen, Terroristen oder sogenannten „Hacktivisten“ ausgenutzt, sondern auch von Staaten und staatlich geförderten Akteuren.

Angriffe aus dem Cyber- und Informationsraum sind schon lange keine Fiktion mehr, sondern Realität. 2017 ließ der Erpressungstrojaner „Wanna Cry“ unter

anderem Anzeigetafeln der Deutschen Bahn ausfallen. Letztes Jahr wurde unser Regierungsnetz IVBB angegriffen, und auch der Deutsche Bundestag blieb nicht verschont.

Klar ist: Deutschland und seine Partner in der EU und NATO sind Ziele von Cyberattacken. Konflikte in der realen Welt werden oftmals auch in den Cyberraum übertragen. Russland zum Beispiel nutzt Cyberangriffe zur umfassenden Informationsbeschaffung und flankiert außen- und sicherheitspolitische Absichten durch Cyber-Operationen. Auch China bedient sich langfristiger und strategisch angelegter Cyberangriffe mit dem Ziel der Aufklärung außen-, sicherheits- und wirtschaftspolitischer Standpunkte und zur Einschätzung von Handlungsoptionen.

Durch Globalisierung und Digitalisierung entstehen also neben den Chancen auch neue Herausforderungen für Gesellschaft, Politik und Streitkräfte. Gefährdungen für unseren Staat und unsere Gesellschaft sind dabei hybrider geworden und zunehmend schwerer zuzuordnen. Potentielle Angreifer nutzen die Möglichkeiten, die sich aus Globalisierung und Digitalisierung ergeben – zumeist befinden sich diese unterhalb der Schwelle der konventionellen Kriegführung. Dementsprechend ist die Landes- und Bündnisverteidigung wesentlich facettenreicher geworden.

Durch Globalisierung und Digitalisierung entstehen neben den Chancen auch neue Herausforderungen für Gesellschaft, Politik und Streitkräfte.

Mit Blick auf die komplexe Bedrohungslage fordert die Bundesregierung im Weißbuch 2016 daher eine gesamtstaatliche Sicherheitsvorsorge, die eine Intensivierung der Zusammenarbeit zwischen staatlichen Organen, Bürgerinnen und Bürgern sowie privaten Betreibern kritischer und verteidigungswichtiger Infrastruktur vorsieht. Das Miteinander aller in der gemeinsamen Sicherheitsvorsorge muss selbstverständlich sein!

Bedrohungen aus dem Cyber-Raum werden sich nie vollständig verhindern lassen. Die Bundesregierung strebt daher einen Zustand an, in dem die Risiken für Deutschland aus dem Cyber-Raum auf ein tragbares Maß reduziert sind. Das bedeutet, dass wir nicht nur die Abwehr von, sondern insbesondere auch den Umgang mit dem gesamten Spektrum von Bedrohungen schnellstmöglich erlernen und kontinuierlich verbessern müssen. Dabei spielt Resilienz eine zentrale Rolle.

Resilienz bezeichnet die Fähigkeit eines Systems, nach einem externen Schock in den Ursprungszustand zurückzukehren oder sich an die durch den Schock verursachte Veränderung anzupassen und seine Kernaufgaben weiterhin zu erfüllen. Auf die Gesamtgesellschaft übertragen bedeutet Resilienz, dass wir dafür Sorge tragen müssen, dass wir als Staat im Krisenfall funktionsfähig bleiben oder schnell wieder funktionsfähig werden.

Präventiv müssen wir uns insbesondere um die kritischen Bereiche kümmern: Energie, Wasser, Gesundheit, Internet, Verkehr oder Finanzströme.

Es geht um den Ausbau der Widerstands- und Adaptionsfähigkeit von Staat und Gesellschaft gegenüber Störungen. Schadensereignisse müssen absorbiert werden können, ohne dass die Funktionsfähigkeit von Staat, Wirtschaft und Gesellschaft nachhaltig beeinträchtigt wird.

Als 2016 die „Konzeption zivile Verteidigung" veröffentlicht wurde, haben Teile der Öffentlichkeit dies als Aufforderung zu Hamsterkäufen verstanden. An diesem Beispiel zeigt sich besonders die Bedeutung öffentlicher Kommunikation, die es der Gesellschaft ermöglicht, Risiko-, Gefahren- und Bedrohungslagen richtig einzuschätzen und gegebenenfalls notwendige individuelle Vorkehrungen zu treffen.

In Sachen Resilienz ist der Staat nicht nur auf sich selbst gestellt, sondern in hohem Maße auf die gesamte Gesellschaft angewiesen, auf eine im besten Sinne „wehrhafte Demokratie", auf gesellschaftliche Selbstbehauptung und auf die Bereitschaft zur Verteidigung unserer freiheitlich-demokratischen Grundordnung.

In Sachen Resilienz ist der Staat nicht nur auf sich selbst gestellt, sondern in hohem Maße auf die gesamte Gesellschaft angewiesen, auf eine im besten Sinne „wehrhafte Demokratie", auf gesellschaftliche Selbstbehauptung und auf die Bereitschaft zur Verteidigung unserer freiheitlich-demokratischen Grundordnung.

Sicherheitsvorsorge und Resilienz sind auch für die Bundeswehr von enormer Bedeutung. Als Nutzer komplexer Technologie ist die Bundeswehr besonders von der Digitalisierung betroffen. Gefordert ist eine Anpassung von Denken und Handeln auf allen Ebenen. Wer digitalisiert, ist schneller und gewinnt! Gerade in diesem Kontext ist es wichtig, die Soldatinnen und Soldaten im Prozess der Gestaltung der Digitalisierung mitzunehmen, denn sie tragen die digitale Transformation der Bundeswehr. Zwar ändern sich der Auftrag und die Aufgaben der Bundeswehr durch Digitalisierung nicht, sehr wohl aber die Art und Weise der Auftragserfüllung. Daher ist die digitale Transformation der

Bundeswehr entscheidend für die Reaktionsfähigkeit und damit essentieller Bestandteil der Fähigkeit zur Landes- und Bündnisverteidigung Deutschlands.

Die Digitalisierung ist deshalb in der Bundeswehr auf allen Ebenen Chefsache. Zentrale strategische Elemente, wie z.B. das Leitungsboard Digitalisierung der Bundesministerin und die Umsetzungsstrategie Digitale Bundeswehr, sind dazu im BMVg bereits etabliert. Dadurch ist eine gute Grundlage für die digitale Transformation gelegt.

Die „Konzeption der Bundeswehr" nimmt für unsere Streitkräfte das Thema „Resilienz" auf und unterscheidet dort zwischen personeller, kognitiver, funktionaler, materieller und organisatorischer Resilienz. Qualifiziertes, leistungs- und reaktionsfähiges Personal in einem flexiblen Personalkörper ist der Kern personeller Resilienz. Eine aufgeklärte und gut informierte Truppe besitzt kognitive Resilienz gegenüber hybriden feindlichen Vorgehensweisen. Einsatzorientierte Ausbildung, die unsere Soldatinnen und Soldaten handlungssicher agieren lässt, stärkt funktionale Resilienz. Eine aufgabenorientierte Vollausstattung ist eine entscheidende Voraussetzung für materielle Resilienz. Eine wesentliche Rolle spielt dabei der für das Fähigkeitsprofil der Bundeswehr maßgebliche Systemverbundgedanke. Im Kern bedeutet dies, dass neben dem Kern einer Fähigkeit immer auch sämtliche erforderlichen Unterstützungselemente von Beginn an mitgeplant werden müssen. Organisatorische Resilienz kann dabei auch durch gezielte Redundanzen in den Strukturen der Bundeswehr erreicht werden, die vor allem eine durchhaltefähige Führungsfähigkeit aufrechterhalten.

Das größer werdende, immer komplexere Spektrum an klassischen und neuen Herausforderungen stellt hohe Ansprüche an den Dienst in der Bundeswehr und fordert ihre Angehörigen in besonderem Maße. Die Soldatinnen und Soldaten ebenso wie die zivilen Mitarbeiterinnen und Mitarbeiter werden durch politische, historische, interkulturelle und ethische Bildung auf ihren Dienst und die damit verbundenen Herausforderungen vorbereitet. Bildung und Weiterbildung sind dabei eine elementare Führungsaufgabe aller Vorgesetzten.

Die Konzeption der Inneren Führung trägt zum Verständnis der Sinnhaftigkeit des Dienstes und des Auftrags bei. Wir qualifizieren unsere Soldatinnen und Soldaten daher nicht nur in historischer und politischer Bildung, sondern auch in ethischen Fragen. Innere Führung leistet so einen wichtigen Beitrag dazu, unsere Soldatinnen und Soldaten resilient gegen Risikofelder zu machen.

Eine zentrale Rolle kommt der Bundeswehr zudem im Bereich des Heimatschutzes zu. Dazu zählen die Aufgaben, die im Rahmen der gesamtstaatlichen Sicherheitsvorsoge zum Schutz Deutschlands und seiner Bürgerinnen und Bürger außerhalb des Spannungs- und Verteidigungsfalls durch die Bundeswehr wahrzunehmen sind.

In Deutschland dürfen die Streitkräfte zur Hilfeleistung bei Naturkatastrophen und besonders schweren Unglücksfällen eingesetzt werden. Die Verfahren dazu sind ständig geübte Praxis. Zur Unterstützung bei besonders schweren Unglücksfällen zählt auch der Einsatz unserer Streitkräfte bei terroristischen Anschlägen katastrophischen Ausmaßes. Die entsprechenden Verfahren werden ebenfalls laufend bei gemeinsamen Übungen mit den Bundesländern zur Terrorismusabwehr geübt.

Die Bundeswehr unternimmt alle Anstrengungen, um den Herausforderungen, die aus Globalisierung und Digitalisierung erwachsen, ausgewogen zu begegnen. Bei Resilienz und Sicherheitsvorsorge spielen unsere Streitkräfte eine zentrale Rolle. Doch Landes- und Bündnisverteidigung sind eine gesamtstaatliche Kraftanstrengung. Deswegen kommt es auf uns alle an. Jede und jeder Einzelne kann sich in den Diskurs vor Ort, in Vereinen und Parteien einbringen und zur Sensibilisierung der Bürgerinnen und Bürger beitragen. Die Verwundbarkeit unserer Institutionen und unserer Infrastruktur zu erkennen und ihr zu begegnen, bleibt eine gemeinsame Aufgabe von Politik und Gesellschaft, die sich dabei auf unsere Streitkräfte verlassen können.

Hinweis: Mehr zum Thema Globalisierung, Digitalisierung und Resilienz siehe Bericht über die 53. Sicherheitspolitische Informationstagung der Clausewitz-Gesellschaft e.V. und der Führungsakademie der Bundeswehr auf den Seiten 231 bis 240.