Lesestoff von Fachleuten für Kenner

Bundeswehr der Zukunft. Verantwortung und künstliche Intelligenz
Schon der Titel des Sammelbandes „Bundeswehr der Zukunft. Verantwortung und künstliche Intelligenz“ kann als wegweisend begriffen werden, zeichnet er doch das Bild einer Zukunft, in der unsere Streitkräfte neu gedacht werden müssen, um in einer Welt voller sicherheitspolitischer Herausforderungen Verteidigungsfähigkeit zu gewährleisten. Die Übernahme von Verantwortung für die Sicherheit Deutschlands und Europas in Zusammenarbeit mit unseren internationalen Bündnispartnern und die Offenheit für die Entwicklung und Etablierung neuer Technologien sind dabei unerlässliche Komponenten einer modernen Bundeswehr.

Was außerdem dazu gehört, führen knapp 40 Autor:innen auf 470 Seiten aus, wobei jedes der neun Kapitel aus mehreren Beiträgen zu einem Oberthema besteht. Zu Wort kommen hochkarätige Expert:innen aus Wissenschaft, Politik und Militär, sodass ein Mosaik aus Perspektiven entsteht, welches sich letztlich zu einem Gesamtbild zusammenfügt, das Einblicke in aktuelle Herausforderungen und Ausblicke auf künftige Potenziale der Bundeswehr gibt.
So äußert sich die Wehrbeauftragte Dr. Eva Högl gemeinsam mit ihrem wissenschaftlichen Mitarbeiter Sebastian Jüngst zur Notwendigkeit, „innere Führung und Künstliche Intelligenz zusammen [zu] denken und [zu] gestalten“, während Dr. habil. Frank Sauer skizziert, wie eine staatliche „Regulierung von Autonomie in Waffensystemen“ aussehen könnte. Flottenadmiral Christian Bock und Major i.G. Mathias Schmarsow äußern sich zu konkreten Einsatzmöglichkeiten von KI in Bezug auf militärische Führung und Entscheidungsfindung. Zu den politischen Implikationen und Handlungsoptionen melden sich die Bundestagsabgeordneten Markus Grübel, Sonja Müller, Dr. Johann Wadepfuhl und Florian Hahn in insgesamt drei Beiträgen zu Wort. Aufschlussreich ist auch der globale Blick, den beispielsweise Dr. Océane Zubeldia hinsichtlich künftiger deutsch-französischer Kooperationen in Sachen KI wagt oder den Dr. Melanie W. Sisson auf die US-chinesischen Beziehungen im hochtechnologisierten Zeitalter wirft.

Empfehlenswert ist das Werk für all jene, die sich interdisziplinär mit aktuellen Herausforderungen und Weiterentwicklungschancen der Bundeswehr – insbesondere mit Blick auf potenzielle Einsatzmöglichkeiten moderner Technologien wie KI – auseinandersetzen wollen. Dabei haben die Autor:innen den Anspruch, ein breites gesellschaftliches Publikum anzusprechen, was sich in einer zugänglichen Sprache äußert.

Ariatani Wolff

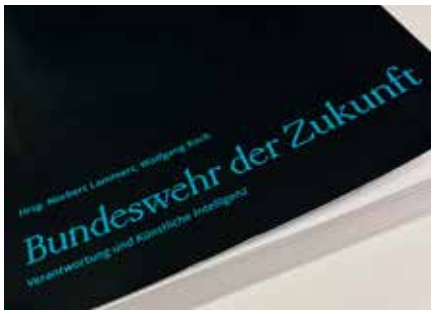

Foto: privat

Landesverteidigung.
Ausgehend von einer allgemeinen Reflexion über die sicherheitspolitischen Herausforderungen von Cyberangriffen für die deutsche Sicherheitsarchitektur wirft dieses Werk die Frage auf, ob die Abwehr von Cyberangriffen durch die Bundeswehr gewährleistet werden sollte. Um dem nachzugehen, arbeitet Maximilian Orthmann eine Definition der Einsatzbefugnisse der Bundeswehr aus: Demnach gehe es nicht darum, eine Modifikation des juristischen Auslegungsbereiches für neue Gefährdungslagen vorzunehmen, sondern bereits bestehende Normen hinsichtlich ihres „korrekten“ Verständnisses zu prüfen.

Um den inhaltlichen Normgehalt der Einsatzbefugnisse zu prüfen, werden im gesamten Werk zentrale Begriffe der Wehrverfassung aufgeschlüsselt. Die Wehrverfassung wird im vorliegenden Werk als die „Gesamtheit aller im wehrrechtlichen Kontext stehenden Normen“ verstanden. Grundsätzlich wird zwischen Einsatzbefugnissen bei Angriffsszenarien mit und ohne militärischer Dimension unterschieden. Sei es für die Darstellung der Struktur des Verteidigungsbegriffs, der Verteidigungslage oder der Verteidigungshandlung – stets wird in juristischer Fachsprache argumentiert und zur Veranschaulichung der rechtlichen Lage auf Abbildungen zurückgegriffen.

Sicher ist der Begriff Verteidigung allen Bürger:innen geläufig. Welche Anforderungen zur legitimen Abwehr von Angriffen dahinterstehen, ist allerdings weit weniger bekannt und wird in diesem Buch beleuchtet. Um nur eine der zahlreichen Begriffsdefinitionen zu betrachten: Verteidigung versteht sich als Abwehr eines Angriffs, der bestimmte Anforderungen erfüllt, das heißt vor allem einen militärischen Bezug aufweist. Letztendlich kommt Orthmann zu dem Schluss, dass die aus der Begrenzung der Einsatzszenarien resultierenden Lücken der wehrverfassungsrechtlichen Einsatzbefugnisse zwar eine Überarbeitung der Streitkräftebefugnisse, jedoch keine Ausweitung derselben verlangen.

Simone Bieringer

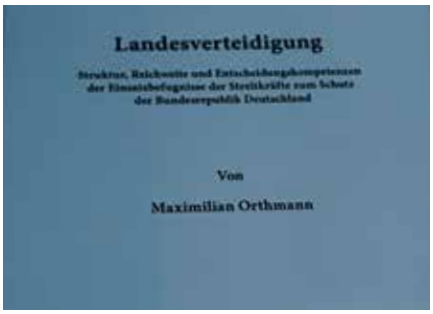

Foto: privat

Das NATO-Cyber-Rapid-Response-Team: Genug für ein ambitioniertes Ziel?

Der digitale Raum hat in den vergangenen Jahren als operatives Feld zunehmend an Bedeutung gewonnen. Immer häufiger verlagern sich Kriegsgeschehen auch in den Cyberraum und von einer klassischen Kriegsführung wenden wir uns verstärkt einer hybriden Kriegsführung zu. Egal ob durch das Verbreiten von desinformativen Inhalten, DDoS-Angriffe (Versuch, eine Netzwerkressource durch Überflutung von Anfragen zum Zusammenbruch zu führen) oder Hackerangriffe, beispielsweise mit dem Ziel, die kritische Infrastruktur eines Landes lahmzulegen: Akteure im Cyberraum operieren mit einem hohen Maß an Kreativität, aber auch mithilfe von ausgeklügelten Verschleierungstaktiken.

Dennoch sind keine dieser Möglichkeiten neu. Vielmehr ist eine Veränderung im Hinblick auf die Qualität sowie auf die Orchestrierung von diversen Instrumenten feststellbar, welche die Sicherheitspolitik von primär demokratischen Staaten auf eine Probe stellt. Allerdings sind Cyberangriffe nicht nur eine Gefahr für demokratische Systeme. Auch für Soldat:innen, die sich beispielsweise in Friedenseinsätzen der UNO befinden oder die (kritische) Infrastruktur von Staaten, können Cyberangriffe in unterschiedlichen Variationen eine große Wirkungsmacht entfalten.

Deshalb hat die NATO im Jahr 2011 mit der Gründung einer neuen Einheit auf diese Gefahren reagiert. Diese ist seit 2012 operativ tätig und nennt sich Cyber Rapid Reaction Team (CRRT). Das CRRT ist an das technische Zentrum der NATO angegliedert und bestand bislang aus sechs ständigen Expert:innen. Je nach Mission wurden zusätzlich nationale oder NATO-Expert:innen hinzugezogen, die das Ziel der Mission unterstützten. Im Zuge des NATO-Gipfels im Juni 2022 wurde jedoch festgestellt, dass die bisherigen Maßnahmen gegen Angriffe aus dem Cyberraum nicht mehr ausreichen. In Madrid wurde verkündet, dass der Aspekt der Cybersicherheit weiterentwickelt werden soll. Diese Weiterentwicklung hat jüngst die deutsche Cyberbotschafterin Regine Grienberger im „Podcast vom Posten" des Auswärtigen Amts angesprochen. Sie kündigte an, dass noch in diesem Jahr die Einrichtung einer schnellen Eingreiftruppe für den Cyberraum erfolgen wird. Ziel der Truppe ist es, bei Cyberangriffen schnell zu reagieren, den betroffen Alliierten zu unterstützen und kritische sowie digitale Infrastrukturen zu schützen.

Die schnelle digitale Eingreiftruppe soll jedoch, wie aus der NATO-Deklaration beim Gipfel 2021 hervorgeht, auf freiwilliger Basis beruhen. Dies wirft die Frage auf, warum sich gegen festere Strukturen innerhalb der NATO entschieden wurde. Sinnvoller wäre es, das schnelle Eingreifteam an das CRRT der NATO anzugliedern, um eine gemeinsame Cyberabwehr aller NATO-Mitgliedsstaaten zu gewährleisten. Ein Problem des Freiwilligkeitsprinzips ist der mögliche Verlust von wichtigen Kenntnissen, sollten sich Staaten nach einiger Zeit gegen eine weitere aktive Partizipation entscheiden. Auch wenn die Ständige Strukturierte Zusammenarbeit der EU (engl. Permanent Structured Cooperation, kurz PESCO), an der sich orientiert werden soll, im Hinblick auf das europäische Cyber Rapid Response Team ebenfalls auf freiwilliger Basis arbeitet, scheint sie dennoch mehr Struktur zu haben. Dem CRRT der EU liegt ein Rotationsprinzip zu Grunde, wie es in ähnlicher Art und Weise auch bei der NATO Response Force (NRF) praktiziert wird. Im jährlichen Abstand wird der Staffelstab an ein anderes Land übergeben, welches die Führung übernimmt. Fehlen solche Strukturen bei der NATO und ihrer schnellen digitalen Eingreiftruppe, könnte sich relativ zügig ein Status quo im Hinblick auf den Umgang mit Bedrohungen im Cyberraum etablieren. Dadurch würde sich wiederrum die Abwehrfähigkeit der NATO und ihrer Alliierten auf Dauer verschlechtern.

Die vermeintlich losen Strukturen einer schnellen digitalen Eingreiftruppe der NATO garantieren eine hohe Ausfallquote im Hinblick auf das Wissens- und Fähigkeitsmanagement, weshalb die Antwort des Gipfels von 2021 auf die Bedrohungen und Gefahren im Cyberraum zu kurz greift und den Eindruck erweckt, dass die NATO auf ebendiese noch keine Antwort zu haben scheint. Ein Nachjustieren der NATO ist hier dringend erforderlich, um die Eingreiftruppe langfristig als erfolgreiche Einheit zu etablieren.

Fabienne Hofmeister

Bildunterschrift