BDSV

Bundesverband der Deutschen
Sicherheits- und Verteidigungsindustrie e.V.

Positionspapier des

Ausschusses Digitale Konvergenz

Hybride Bedrohungslage, Handlungsunsicherheit und unterschiedliche Geschwindigkeiten erschweren dringend nötige „Digitale Konvergenz“

September 2023

I. Digitale Konvergenz ist unabdingbar

Der Begriff der „Digitalen Konvergenz“ wurde bereits vor Jahren im BDSV geprägt und ist seither auch das Markenzeichen des jährlich in Berlin stattfindenden, zusammen mit der AFCEA Bonn e.V. organisierten „Konvents zur Digitalen Konvergenz“. Zum diesjährigen 5. Konvent soll der vorliegende Essay Denkanstöße bieten.

Kern „Digitaler Konvergenz in der SVI“ ist: Das reibungslose Zusammenlaufen von Spitzentechnologie für Rüstungs-Plattformen mit einer Spitzenausstattung bei deren Digitalisierung. Nur wenn beide Elemente reibungslos und zeitgleich „konvergieren“, kann das Ziel von Rüstung erreicht werden, nämlich die jeweilige Truppe mit Gerät auszustatten, das ihr die Erfüllung ihrer anspruchsvollen Aufgaben ermöglicht. Diese Aufgaben haben sich für Deutschland und die Bundeswehr durch die „Zeitenwende“ im Februar 2022 nochmals maßgeblich verändert. Es gibt nun – trotz weiterlaufender internationaler Missionen – einen unbedingten Vorrang für Landes- und Bündnisverteidigung und für die der NATO zugesagten Beiträge zur Abschreckung möglicher Angriffe auf NATO-Territorium im Osten Europas.

Aus der Einsicht heraus, dass trotz aller Bemühungen um eine europäische Friedensordnung mit dem Angriff Russlands auf die Ukraine wieder Krieg in Europa herrscht, hat sich zugleich für uns als Gesellschaft der Friedenszustand relativiert. Zwar sind wir nicht unmittelbar Kriegspartei; jedoch sehen wir die Ukraine auch als Verteidigerin unserer freiheitlichen Lebensweise in ganz Europa, die unserer vollen Unterstützung bedarf. Nicht von ungefähr schafft diese Situation auch ein geschärftes Bewusstsein für die Gefahren sog. hybrider Bedrohung. Diese ist mit einer massiven Zunahme an Cyberattacken unübersehbar, jedoch keineswegs als überraschend anzusehen. Unter diesen Aspekten kommt „Digitaler Konvergenz“ eine deutlich gestiegene Bedeutung zu, was in diesem Essay vor allem unter drei Aspekten beleuchtet werden soll.

II. Erster Aspekt: Digitale Konvergenz bei der aktuellen Ausrüstung der Bundeswehr

Die „Zeitenwende“ führt zu unmittelbar gestiegenen Ansprüchen an die Ausrüstung der Bundeswehr, die sich nicht zuletzt in der Genehmigung des Sondervermögens von 100

Mrd. € durch den Deutschen Bundestag manifestiert haben. Laut Angabe von BMVg/BAAINBw werden bis zum Jahresende 2023 zwei Drittel des Sondervermögens durch Verträge gebunden sein.[1] Bezeichnenderweise trifft diese Feststellung jedoch am wenigsten auf die 20,8 Mrd. €[2] zu, die innerhalb des Sondervermögens für Digitale Führungsfähigkeit vorgesehen sind. Allein dies führt das Problem unterschiedlicher Geschwindigkeiten und mangelnder Konvergenz bei klassischer Rüstung und ihrer entsprechenden Digitalisierung vor Augen. Eine stärkere Einbindung der an sich komplex integrierten Wirkmittelsysteme (also Fahrzeug, Flugzeug, Schiff, Informationstechnologie, etc.) in den übergreifenden Informations- und Wirkverbund mittels Informationstechnologie stärkt letztendlich Führungs- und Wirkungsfähigkeit. Konkret betrifft dies vor allem die seit Langem überfällige Digitalisierung Landbasierter Operationen (D-LBO), deren mehrfache konzeptionelle Rückschläge nun die Bereitstellung der für 2025 versprochenen voll-digitalisierten Heeres-Division gefährden.

Bei den weiteren großen Projekten aus dem Sondervermögen der 20,8 Mrd. € (Führungsfähigkeit und Digitalisierung wie etwa SATCOMBw Stufe 2 und 3, TaWAN, GMN 1 & 2) ist ein Vertragsschluss vermutlich ebenfalls erst in 2024 zu erwarten wie sich aus dem vom Kabinett beschlossenen Haushaltsplan 2024 mit mittelfristigem Finanzplan bis 2027 entnehmen lässt. Eine deutliche Beschleunigung in diesem Bereich, wie etwa bei Munition und Waffensystembeschaffung, ist damit in höchstem Maße notwendig, um das Gesamtsystem der vernetzten Operationsführung rechtzeitig zu realisieren.

III. Zweiter Aspekt: Handlungsunsicherheit angesichts steigender hybrider Bedrohung und mangelnder Resilienz

Seit Jahren ist die Notwendigkeit erkannt, die Fähigkeiten zur Aufklärung im Cyber- und Informationsraum und zur Abwehr von Schäden durch Informations- und Cyber-Operationen ausbauen zu müssen. Auf Seiten der Bundeswehr wurde das Kommando Cyber- und Informationsraum aufgestellt und strukturell weiterentwickelt. Eine zielführende gesamtstaatliche Umsetzung, insbesondere die Ausprägung moderner Analyseverfahren auf Basis vertrauenswürdiger Technologien und resiliente Prozessvernetzung der

[1] Siehe https://www.faz.net/aktuell/wirtschaft/beschaffungsamt-der-bundeswehr-falsche-zusagen-aus-der-industrie-19108968.html
[2] Siehe https://www.bundesregierung.de/breg-de/themen/sicherheit-und-verteidigung/sondervermoegen-bundeswehr-2047518

relevanten Stellen der Inneren und äußeren Sicherheit samt Industrie, erfolgt nur unzureichend.

Die durch Digitalisierung und Innovation getriebene Konvergenz der analogen und digitalen Welt in Gesellschaft und kritischen Infrastrukturen nimmt stetig zu; auch deshalb wird das Thema Cybersicherheit und kognitive Resilienz immer wichtiger. Zur Verteidigung gegen Angriffe auf Leib und Leben statten wir unsere staatlichen Sicherheitsorgane auf Landes- und Bundeseben in den Bereichen der inneren wie der äußeren Sicherheit mit wirksamen Mitteln zur Prävention und zur Schadensbekämpfung aus. Im Cyberraum hingegen erscheinen weder die Rechts- und Verwaltungslage noch die daraus resultierende Mandatierung von Fähigkeiten zur Abwehr von Schäden an Leib und Leben der Bevölkerung wie auch der kritischen Infrastrukturen ausreichend ausgeprägt. Zum einen fehlt es an konvergenten Resilienz-Anforderungen als Grundlage für den Aufbau von Verteidigungsressourcen und dazu notwendiger industrieller Fähigkeiten. Zum anderen sind gerade bei Angriffen aus bzw. im Cyberraum die Fähigkeiten zur Erkennung und Abwehr solcher Angriffe unzureichend ausgeprägt. Praktikable Vorgehensweisen, um zeitgerecht eine akzeptable Schadensminimierung gewährleisten zu können, sind hier nicht ausreichend definiert. Dies gilt umso mehr dann, wenn die Wirkung digitaler Angriffe sich in der analogen Welt niederschlägt (wie beim Ausfall von Energieversorgung).

Bisher unterscheiden sich die rechtlich vorgegebenen Verfahrensweisen bei Angriffen in der analogen und digitalen Welt signifikant: In der analogen, physischen Welt wird primär versucht, Schaden abzuwenden und Bedrohten oder Verletzten zu helfen. In der digitalen Welt wird stattdessen zuerst eine Attribuierung gefordert, um dann entscheiden zu können, ob der Angriff in die Zuständigkeit der inneren Sicherheit auf Bundes- oder Landesebene oder der äußeren Sicherheit fällt. Zwar wird in der digitalen Welt eine grundsätzliche Härtung und Absicherung kritischer nationaler Infrastrukturen durch entsprechende Mindeststandards gefordert; die regulatorische Umsetzung ist bisher jedoch nicht ausreichend ausgeprägt. Erschwert wird Verteidigung in der digitalen Welt außerdem durch die Auflösung von Grenzen zwischen privaten und öffentlichen Bereichen der Informationsversorgung und Meinungsbildung. Aufgrund vielfach herrschender Anonymität gestaltet sich die Zuordnung von Angriffen zu Verursachern sowie zeitlichen und

räumlichen Anknüpfungspunkten schwierig bis unmöglich. Erforderlich sind zusätzliche Kompetenzen, Ressourcen und eine erhöhte Geschwindigkeit in den Prozessen.

Fazit: Die zunehmend dynamischeren Lagen lassen die historisch gewachsene binäre Unterscheidung vom Friedens- und Kriegszustand als nicht mehr ausreichend erscheinen. Vielmehr stellen sie neue Anforderungen an die auf den Friedensgrundbetrieb ausgerichteten Verwaltungsstrukturen, auch in Form neuartiger Kooperationsmodelle zwischen Behörden und Industrie, um so den Herausforderungen zum Schutz gegen Cyberangriffe gewachsen zu sein. Dabei müssen für die Organe der öffentlichen Sicherheit – wie z.B. Polizei, Bundeswehr und Nachrichtendienste - klare Definitionen, Maßstäbe und Verhaltensregeln festgelegt werden, wie sie in Gestalt der im Jahr 1989 erlassenen „Gesamtverteidigungs-Verordnung“ unter anderen äußeren Voraussetzungen schon einmal implementiert worden waren.

Die Bedrohungen und Herausforderungen, denen Deutschland gegenübersteht, können sich schnell und unvorhersehbar entwickeln. Sie können verschiedene Aspekte wie militärische, politische, wirtschaftliche, technologische oder umweltbezogene Faktoren umfassen. Gerade unter großem sicherheitspolitischem Druck wird es in einer solchen Umgebung schwierig sein, die nach unserer Rechtsordnung gebotenen klaren Unterscheidungen zwischen Frieden, Spannungsfall, Krisenfall und Verteidigungsfall zu treffen. Daher erscheint es wichtig, flexiblere und dynamischere Ansätze zu entwickeln, um auf Bedrohungen und Herausforderungen zu reagieren. Dies erfordert eine enge Zusammenarbeit zwischen den Streitkräften, zivilen Behörden und anderen relevanten Akteuren sowie die Bereitstellung notwendiger Fähigkeiten und Ressourcen. In einer solchen Umgebung kann die Grauzone zwischen Frieden und Konflikt sehr schmal sein, und es kann schwierig sein, schnell und angemessen auf unvorhergesehene Entwicklungen zu reagieren.

Bezogen auf die Dimension Wirtschaft bzw. Rüstungswirtschaft geht es primär um eine auf die jeweils vorhandene Bedrohungslage abgestimmte Versorgung der Gesellschaft und der Industrie. Gleichermaßen sind sowohl die Versorgungsketten für die Bevölkerung mit Nahrungsmitteln, Verbrauchsgütern und sicheren Kommunikationswegen zu betrachten

wie auch die Versorgung der Institutionen zum Beispiel im Bereich der BOS mit entsprechenden sicheren Betriebsmitteln (Lieferketten). Ein besonderes Augenmerk liegt hierbei auf der Energieversorgung sowie der Versorgung der Industrie mit Produktionsgütern und kritischen Rohstoffen sowie ggfs. knappen Vorprodukten (Stichwort: Halbleiter). Immer stellt sich dabei auch die Frage der Priorisierung im Vorfeld eines festgestellten Verteidigungsfalles, also bevor das Ordnungsprinzip der „Kriegswirtschaft“ alle anderen Bedarfe den Bedürfnissen der Verteidigungsindustrie unterordnet.

IV. Dritter Aspekt: Bedrohung Digitaler Konvergenz durch einschränkende Regulatorik

Digitale Konvergenz bedeutet im wirtschaftlichen Kontext – bedingt durch neue Digitalisierungstechnologien – das Entstehen neuer Nutzeranforderungen mit der Folge sich verändernder Potentiale, Märkte und Wertschöpfungsketten. Im Rahmen sicherheits- und verteidigungstechnologischer Fähigkeiten weitet sie damit zugleich auch den sicherheitspolitischen Horizont. Der massiv ansteigende Einsatz von sog. schwacher und starker Künstlicher Intelligenz (KI) im Bereich der Verteidigungstechnologien bietet hierfür vielfaches Anschauungsmaterial. Auch hieraus wird deutlich, dass sich Sicherheit und Verteidigung nicht mehr nur in rüstungspolitischen Kontexten manifestieren, sondern weit darüber hinaus mit einer Vielzahl politischer, insbesondere auch gesellschaftspolitischer Kontexte verbunden sind, die den Begriff der Sicherheitspolitik weiten. Hiervon ausgehend entwickeln EU und Bundesregierung jedoch eine Regulatorik, die den spezifischen sicherheits- und verteidigungspolitischen Zusammenhang vielfach zu wenig im Blick hat. Dies betrifft vor allem den Digitalisierungsbereich und schränkt die Möglichkeiten der Industrie, angemessen konvergente Technologien für unsere staatlichen Sicherheitsorgane und Streitkräfte zu entwickeln, mitunter empfindlich ein. Die Folge daraus wird sein, dass in immer mehr Bereichen digital konvergente Rüstungsgüter aus Ländern wie USA und Israel beschafft werden (s. jüngst Heron TP oder Arrow 3).

Auf der EU-Ebene zeigt das Beispiel des „AI-Act“, wie moralisch gut gemeinte Verbote im Bereich militär- und sicherheitsrelevanter KI, etwa im Bereich der Erkennung und Nutzung personenbezogener Merkmale, die Gefahr begründen, dass die europäische Industrie von der Entwicklung und Nutzung entsprechender Daten für sicherheitsbezogene Zwecke

abgekoppelt und dadurch die Tendenz zur Beschaffung im Nicht-EU-Ausland weiterbefördert wird.

Deutschland ist wohl das einzige Land der EU, das die DSGVO sowie die daraus folgenden Regelwerke zugleich komplett auch auf die eigenen Sicherheitsbehörden anwendet. Unter der Kontrolle des Bundesbeauftragten für Datenschutz führt dies bei den Sicherheitsbehörden zu signifikant höheren Aufwänden als dies auf Seiten der Industrie der Fall ist. Hinzu kommen die unterschiedlichen Gesetze zwischen Bund und Ländern. Eine Ausnahme bildet Luftsicherheit, während Küstenschutz und erst recht Cyber in dieser Hinsicht Probleme bereiten. Diese Probleme betreffen nicht nur die Einhaltung von DSGVO, BDSG, LDSGen, sondern auch den eingeschränkten Informationsaustausch zwischen Sicherheitsbehörden, durch den eine vernetzte Analysefähigkeit stark verkompliziert wird. Durch die Industrie bereitgestellte Lösungen, die jene deutsche Regulatorik erfüllen, sind in ausländischen Märkten zwar respektiert, aber gegenüber Mitbewerberprodukten z.B. aus Israel und USA selbst bei höherer Leistungsfähigkeit aufgrund der regulierungsbedingten Komplexität/Kosten selten wettbewerbsfähig.

V. Zusammenfassung: industrielle Forderungen bzw. Empfehlungen

Die gegenwärtige Realität hat viele Denk- und Verfahrensweisen überholt. Die letzten Monate haben gezeigt, dass wir nicht ausreichend vorbereitet waren und sind für das Bedrohungsspektrum und die Konvergenz der Bedrohungsfelder. Die hybriden Szenarien sind nichts anderes als „Digitale Konvergenz“ auf der Seite der Angriffsvektoren. Dem kann nur eine „Digitale Konvergenz“ auf der Seite unserer Sicherheitsorganisationen und -technologien entgegenwirken. Es ist somit erforderlich, dass

- Rüstungsgüter insgesamt so geplant und realisiert werden, dass der Notwendigkeit digitaler Konvergenz entsprechend der Dynamik digitaler Entwicklungen Rechnung getragen wird;

- das gesamte Fähigkeitsspektrum der Verteidigung gegen hybride Bedrohungen so ausgebaut wird, dass digitale Führungs- und Wirkungsfähigkeiten mit den klassischen Verteidigungsfähigkeiten Schritt halten können (insbesondere aufgrund

der Komplexität ist hier ein kollaboratives Vorgehen entlang resilienter Vertrauensketten von Sicherheits- und Verteidigungsindustrie, IT-Industrie und Staat erforderlich);

- das entsprechende Ökosystem - bestehend aus Staat, Sicherheitsbehörden, Sicherheits- und Verteidigungsindustrie und Bevölkerung - resilienter in Bezug auf hybride Bedrohungsszenarien wird (wobei darauf hinzuarbeiten ist, dass wir uns auch in der „Grauzone“ zwischen Frieden und Verteidigungsfall auf unsere eigene Handlungssicherheit verlassen und die begrenzten vorhandenen Ressourcen möglichst effektiv und effizient nutzen können);

- wir nicht durch selbst-induzierte Überregulierung „abgehängt“ werden;

- bei regulativen Vorhaben die Verteidigungsfähigkeit auf Landes- und Bündnisebene - und damit auch die Leistungsfähigkeit der dabei unterstützenden Industrie - ein wesentlicher Bestandteil der Überlegungen werden muss.