

Grundsatzpapier Digitale Verteidigungs- fähigkeit 2026

Nur wer auch wirksam digitalisiert, schafft
Verteidigungsfähigkeit

Auf einen Blick

Grundsatzpapier Digitale Verteidigungsfähigkeit 2026

Ausgangslage

Deutschland muss seine Verteidigungsfähigkeit bis 2027/2028 deutlich schneller stärken. Digitalisierung ist dafür der zentrale Hebel, doch Beschaffung, Integration und Skalierung bleiben zu langsam. Das vorliegende Grundsatzpapier des Bitkom AK Verteidigung benennt die zentralen technologischen, organisatorischen und finanziellen Hebel, um digitale Fähigkeiten schneller in die Truppe und in operative Wirkung zu bringen.

Das Wichtigste

Aus Sicht des Bitkom-AK Verteidigung sind insbesondere drei Handlungsfelder entscheidend:

- **Zeit, Wirkung und Fähigkeiten priorisieren**

Haushalt, Planung und Steuerung müssen sich an konkreten Fähigkeitszielen und operativer Wirkung ausrichten. Digitale Schlüsseltechnologien wie Künstliche Intelligenz, offene Schnittstellen, Datenverarbeitung, 5G und vernetzte Systeme sind strukturell zu priorisieren und durch ein kontinuierliches Fähigkeitsmonitoring messbar zu machen.

- **Beschaffung und Innovation beschleunigen**

Digitale Fähigkeiten müssen in Wochen statt in Jahren in die Truppe gelangen. Dafür braucht es agile Realisierungswege, kürzere Vergabeverfahren, mehr Freiräume für Innovationsakteure sowie eine enge Verzahnung von Entwicklung, Erprobung, Zertifizierung und Einsatz.

- **Skalierung und Resilienz von Beginn an sichern**

Skalierungsfähigkeit, Energieresilienz und digitale Interoperabilität müssen feste Kriterien in Architektur, Beschaffung und Fähigkeitsplanung werden. Zugleich sind industrielle Kapazitäten, privates Kapital sowie die Zusammenarbeit von Bundeswehr, Wirtschaft und Behörden frühzeitig einzubeziehen.

Inhalt

Einleitung	4
1. Digitale Schlüsseltechnologien priorisieren	4
2. Fähigkeiten in den Mittelpunkt stellen	4
3. Beschaffung drastisch beschleunigen	5
4. Innovation in Wirkung überführen	5
5. Skalierung parallel zur Entwicklung sicherstellen	5
6. Kapital und Innovation mobilisieren	6
7. Energie-Resilienz als Grundlage digitaler Verteidigungsfähigkeit	6
8. Gesellschaftliche Resilienz als Voraussetzung stärken	7
Fazit	8

Einleitung

Die sicherheitspolitische Lage erfordert mutige Entscheidungen von der Politik, der Bundeswehr und der Wirtschaft. Verteidigungsfähigkeit entscheidet sich heute nicht mehr an der Höhe der Mittel, sondern an der Geschwindigkeit, mit der Daten zur Definition von souveränen Fähigkeiten und diese in Wirkung überführt werden. Das Zeitfenster bis 2029 ist eng. Entscheidend sind einsatzbereite Fähigkeiten bis 2027/2028. Digitalisierung ist dafür der zentrale Hebel, ihre Bedeutung ist inzwischen unstrittig. Zugleich müssen Abhängigkeiten durch die Stärkung nationaler Wertschöpfungs- und Lieferketten reduziert und die Innovationskraft erhöht werden. Die eigentliche Herausforderung liegt deshalb in der konsequenten Umsetzung, Integration und Skalierung. Was jetzt nicht priorisiert wird, könnte möglicherweise zu spät kommen. Aus Sicht des Bitkom Arbeitskreises Verteidigung zählen nun vor allem Zeit, Wirkung und Umsetzung.

1. Digitale Schlüsseltechnologien priorisieren

- Digitale Führungsfähigkeit entsteht aus der Priorisierung zentraler Technologien. Die Erfahrungen aus der Ukraine sowie die Einschätzungen der Industrie zeigen klar: Offene Schnittstellen, Möglichkeiten zur Aufbereitung, Verarbeitung und zum Austausch von Daten, Künstliche Intelligenz, digitale Infrastrukturen wie beispielsweise 5G sowie Kommunikationstechnologien für vernetzte Systeme und unbemannte Plattformen sind die entscheidenden technischen Treiber militärischer Fähigkeiten. Bereits heute sehen 73 Prozent der Unternehmen Software Defined Defense und 68 Prozent Künstliche Intelligenz als wichtigste Technologien im Verteidigungssektor.
- Die Mittelverwendung im **Verteidigungshaushalt sollte konsequenter an diesen Technologien ausgerichtet werden**. Ziel muss es sein, dass eine solche Priorisierung 2026 auch strukturell im Haushalt und in der Fähigkeitsplanung verankert und sichtbar ist.

73%

der Unternehmen
sehen Software Defined
Defense als eine der
wichtigsten
Technologien im
Verteidigungssektor.
Bitkom-Studie (2025)

2. Fähigkeiten in den Mittelpunkt stellen

- Die zentrale Schwäche der aktuellen Haushaltsstruktur liegt in der fehlenden Verknüpfung von Mitteln und Wirkung. Trotz eines Verteidigungshaushalts von über 600 Milliarden Euro bis 2029 **fehlt es an einer klaren Zuordnung von Investitionen zu konkreten Fähigkeiten**. Der Anteil der Ausgaben für Digitalisierung und Zukunftstechnologien in den vergangenen Jahren lag lediglich bei etwa fünf bis neun Prozent.¹
- Die Mittelverwendung im **Verteidigungshaushalt sollte konsequenter an diesen Technologien ausgerichtet werden**. Ziel muss es sein, dass eine solche Priorisierung 2026 auch strukturell im Haushalt und in der Fähigkeitsplanung verankert und sichtbar ist.

¹ Eigene Berechnungen auf Grundlage der Haushalte der letzten Jahre; siehe auch Schularick & Binder (03/2026): »Time to Spend Smart: Ökonomische Leitlinien für kluge Verteidigungsausgaben«, Kiel Institut für Weltwirtschaft.

3. Beschaffung drastisch beschleunigen

- Die aktuellen Beschaffungszyklen sind mit dem Zieljahr 2029 nicht vereinbar. Während klassische Großsysteme häufig erst nach Jahren verfügbar sind, müssen digitale Fähigkeiten innerhalb deutlich kürzerer Zeiträume Wirkung entfalten.
- Dafür sind **agile Realisierungswege und andere Beschaffungsmechanismen für digitale Fähigkeiten** auszubauen und Standardlaufzeiten signifikant zu reduzieren. **Digitale Fähigkeiten sollten innerhalb von ein bis zwei Monaten in die Truppe gebracht werden können**, teils deutlich schneller, um so unmittelbare operative Wirkung zu erzielen. Einführungsprojekte sollten eng begleitet werden, um deren Effektivität sicherzustellen. Beispielsweise sollten wettbewerbliche Beschaffungsverfahren, wie sie bei Loitering-Munition-Systemen zum Einsatz kamen, sowie vertraglich verankerte Innovationsklauseln künftig häufiger genutzt werden.

4. Innovation in Wirkung überführen

- Eine zentrale Lehre aus der Ukraine ist, dass Innovation nicht nur im Planungsprozess, sondern insbesondere im Einsatz entsteht. Entscheidend ist die Geschwindigkeit, mit der Technologien entwickelt, erprobt und integriert werden. Dabei darf nicht länger die (Beschaffungs-)Prozesssicherheit im Vordergrund stehen, sondern der Mehrwert. Das Innovationszentrum der Bundeswehr muss als Ansprechpartner, Verprobungs- und Zertifizierungsstelle sowie als Vergabestelle schnell das entsprechende Mandat einschließlich Budget erhalten. Die Cyberagentur und der Cyber Innovation Hub müssen durch Entbürokratisierung und mehr Flexibilität in der Erfüllung ihrer Aufträge in ihrer Wirksamkeit weiter gestärkt werden.
- Entwicklung, Erprobung und Einsatz sollten daher deutlich enger verzahnt werden. Ukraine-Erfahrungen und bestenfalls Datenbestände aus diesem Konflikt sollten systematisch genutzt und neue Technologien kontinuierlich in die Truppe integriert werden. Innovation darf nicht punktuell, sondern muss als dauerhafter Prozess organisiert werden. Die **Innovationsakteure im Geschäftsbereich des BMVg sollten weiter gestärkt** werden.

5. Skalierung parallel zur Entwicklung sicherstellen

- Technologische Überlegenheit entsteht nicht allein durch Innovation, sondern auch durch deren breite Verfügbarkeit, durch ein entsprechendes Nutzungsverständnis bei den Soldatinnen und Soldaten sowie durch zivil-militärische Zusammenarbeit. Aktuelle Konflikte zeigen, dass die Fähigkeit zur schnellen Skalierung entscheidend für militärische Wirkung ist. Dies gilt insbesondere für militärische Kommunikationsarchitekturen. Sie werden nur dann skalierbar, wenn spezifische militärische Kommunikationslösungen von Beginn an mit standardisierten zivilen Technologien und Kommunikationsstandards, insbesondere 3rd Generation Partnership Project (3GPP) und 5G, kombiniert und entsprechend weiterentwickelt werden.

- Industrielle **Produktionskapazitäten müssen frühzeitig in die Planung einbezogen werden**. Systeme dürfen nicht nur entwickelt, sondern müssen entweder in großer Stückzahl verfügbar gemacht werden. Alternativ muss, je nach Bedarf, eine ausreichende Produktionskapazität für ihre dynamische und skalierte Nutzung gesichert werden. **Skalierungsfähigkeit sollte dabei als zentrales Kriterium in der Beschaffung** etabliert werden.
- Skalierung ist auch eine Frage der Architektur und der Änderungsfähigkeit. Erforderlich ist eine »Composable-Architektur«, in der Kernfähigkeiten, z. B. in der Logistik, im Personalwesen und in der Instandhaltung, modular kombiniert werden können. So können Fähigkeiten, bei Bedarf mit »Eigenleistungsfähigkeit« ohne vollständige Neuentwicklung, in Wochen anstatt in Jahren angepasst werden.
- Betrieb, Integration und Entscheidungsfähigkeit von Beginn an sicherstellen. Bereits während der Entwicklung müssen die erforderlichen personellen und organisatorischen Ressourcen, Betriebsprozesse und Zuständigkeiten für die spätere Nutzung mitgedacht und mit jedem Entwicklungsschritt weiterentwickelt werden. Abläufe sollten möglichst automatisiert und neue Lösungen von Beginn an in das Gesamtsystem der Bundeswehr integrierbar sein. Zugleich müssen militärische Entscheidungs- und Kommunikationswege so ausgestaltet werden, dass Informationen schnell verarbeitet und Entscheidungen effizient getroffen werden können.

6. Kapital und Innovation mobilisieren

- Die Entwicklung und Skalierung digitaler Verteidigungsfähigkeiten erfordern neben öffentlichen Mitteln auch eine **stärkere Mobilisierung privaten Kapitals**. Insbesondere im Bereich DefTech besteht erhebliches Potenzial, das noch besser genutzt werden kann.
- Der Zugang zu Wagniskapital muss verbessert und neue Finanzierungs- und Kooperationsmodelle etabliert werden. Ziel ist es, die **Wachstumsfinanzierung für innovative Unternehmen nachhaltig zu sichern**. Positiv sind daher die angekündigte Weiterentwicklung des Zukunftsfonds um ein Direktbeteiligungsvehikel für Defense-Startups, wie in der Startup- und Scaleup-Strategie des Bundes angekündigt, sowie die Öffnung von KfW Capital für Investitionen in junge Wachstumsunternehmen der Sicherheits- und Verteidigungsindustrie. Beide Schritte können dazu beitragen, mehr privates Wachstumskapital für DefTechs zu mobilisieren.

7. Energie-Resilienz als Grundlage digitaler Verteidigungsfähigkeit

- **Digitale Verteidigungsfähigkeit setzt eine belastbare und resiliente Energieversorgung voraus**. Führungsinformationssysteme, Kommunikationsnetze, Rechenzentren, Sensorik, Künstliche Intelligenz und autonome Systeme können nur dann Wirkung entfalten, wenn sie auch unter Krisen-, Angriffs- und Ausfallbedingungen dauerhaft mit Energie versorgt werden. Aktuelle Konflikte zeigen, dass Energie- und Versorgungsinfrastrukturen zu den prioritären Angriffszielen moderner Kriegsführung gehören. Die Fähigkeit zum autonomen

Betrieb kritischer militärischer und verteidigungsrelevanter Infrastrukturen im Ernstfall muss daher als eigener Bestandteil nationaler Verteidigungsfähigkeit verstanden werden.

- **Energieresilienz sollte künftig systematisch in Planung, Beschaffung und Digitalisierung berücksichtigt werden.** Neben dem Schutz kritischer Energieinfrastrukturen umfasst dies insbesondere Transparenz über Energieverbräuche und -abhängigkeiten, die Fähigkeit zur Aufrechterhaltung des Betriebs unter Krisenbedingungen sowie die Verringerung strategischer Verwundbarkeiten. Ziel ist eine höhere operative Durchhaltefähigkeit und eine stärkere Unabhängigkeit gegenüber externen Störungen und Angriffen.

8. Gesellschaftliche Resilienz als Voraussetzung stärken

- Verteidigungsfähigkeit ist eine gesamtstaatliche Aufgabe. Militärische Wirkung ist dabei eng mit der Funktionsfähigkeit von Staat, Wirtschaft und kritischen Infrastrukturen verbunden. Beispielsweise zeigt die Bitkom-Studie zu hybriden Angriffen, dass Unternehmen bei Ausfällen zentraler digitaler Infrastrukturen nur begrenzt handlungsfähig sind.
- Kritische Infrastrukturen, Datenverfügbarkeit und Kommunikationssysteme sollten daher gezielt abgesichert werden. Gleichzeitig ist die **Vernetzung zwischen Bundeswehr, Wirtschaft und Behörden auszubauen**. Hierzu sollten öffentliche Akteure noch stärker informieren und gemeinsame Formate anbieten. Neben resilienten Strukturen braucht es für gesellschaftliche Resilienz auch eine informierte Gesellschaft. Dazu gehören niedrigschwellige Informationsangebote, die über hybride Bedrohungen, Desinformation, Vorsorgemöglichkeiten und das richtige Verhalten im Krisenfall aufklären. In Verbindung mit gezielter Aufklärung kann die Gesellschaft so dabei unterstützt werden, manipulierte Inhalte zu erkennen. Damit lässt sich auch die gesellschaftliche Widerstandsfähigkeit gegenüber Desinformation stärken.
- Die Vernetzung von Bundeswehr, zivilen Behörden und der Wirtschaft scheitert im Krisenfall häufig an fehlender digitaler Interoperabilität. Amtshilfeersuche, Logistikketten und Lageberichte werden noch per E-Mail koordiniert. Wirksame Resilienz erfordert eine behördenübergreifende Case-Management-Fähigkeit, die Vorgänge medienbruchfrei, revisionssicher und priorisierbar macht.
- Parallel zur Absicherung kritischer Infrastrukturen muss die Verbesserung der digitalen Souveränität Ziel des Schulterschlusses zwischen der Politik und der Wirtschaft sein. Als wesentliche Voraussetzung für Verteidigungsfähigkeit müssen souveräne Soft- und Hardwarelösungen im Bündnisraum sichergestellt werden. Grundlagen dafür sind die Schaffung positiver politischer Rahmenbedingungen, strategische Kooperationen zur Verfolgung gemeinsamer politischer Interessen sowie ein wirtschaftliches Ökosystem für die konkrete Bedarfsdeckung und die Stärkung von Anbieter- und Produktvielfalt.

Fazit

Wirksame selbstbestimmte Digitalisierung ist eine notwendige Voraussetzung für Verteidigungsfähigkeit. Entscheidend ist dabei nicht die Höhe der Mittel, sondern die Geschwindigkeit, mit der digitale Fähigkeiten in operative Wirkung überführt werden. Zeit und Wirkung sollten die zentralen Faktoren moderner Verteidigungsfähigkeit sein:

Was heute nicht priorisiert, finanziert und umgesetzt wird, entfaltet morgen keine abschreckende Wirkung. Die Herausforderungen sind klar: Digitale Technologien müssen schneller integriert, Innovationen konsequenter skaliert und Fähigkeiten messbarer gemacht werden. Gleichzeitig zeigt die sicherheitspolitische Realität, dass Konflikte längst im Informationsraum, im Cyberraum und auf dem Gefechtsfeld gleichzeitig entschieden werden. Nun gilt es, diese Herausforderungen im Zusammenspiel von Wirtschaft, Bundeswehr und Politik noch besser zu meistern. Wer nicht digital führend ist, wird in diesen Konflikten nicht bestehen können.

Verteidigungsfähigkeit und Resilienz entstehen dort, wo Digitalisierung rechtzeitig Wirkung entfaltet – in der Truppe, in der Infrastruktur und im gesamten staatlichen und wirtschaftlichen System.

Bitkom vertritt mehr als 2.200 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie generieren in Deutschland gut 200 Milliarden Euro Umsatz mit digitalen Technologien und Lösungen und beschäftigen mehr als 2 Millionen Menschen. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 700 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig, kreieren Content, bieten Plattformen an oder sind in anderer Weise Teil der digitalen Wirtschaft. 82 Prozent der im Bitkom engagierten Unternehmen haben ihren Hauptsitz in Deutschland, weitere 8 Prozent kommen aus dem restlichen Europa und 7 Prozent aus den USA. 3 Prozent stammen aus anderen Regionen der Welt. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem leistungsfähigen und souveränen Digitalstandort zu machen.

Herausgeber

Bitkom e.V.

Albrechtstr. 10 | 10117 Berlin

Ansprechpartner

Nemo Buschmann | Referent Öffentliche Sicherheit & Verteidigung

T 030 27576-101 | n.buschmann@bitkom.org

Benjamin Spindeldreier | Junior Manager DefTech & Sicherheit

T +49 30 27576-379 | b.spindeldreier@bitkom.org

Verantwortliches Bitkom-Gremium

AK Verteidigung

Copyright

Bitkom 2026

Diese Publikation stellt eine allgemeine unverbindliche Information dar. Die Inhalte spiegeln die Auffassung im Bitkom zum Zeitpunkt der Veröffentlichung wider. Obwohl die Informationen mit größtmöglicher Sorgfalt erstellt wurden, besteht kein Anspruch auf sachliche Richtigkeit, Vollständigkeit und/oder Aktualität, insbesondere kann diese Publikation nicht den besonderen Umständen des Einzelfalles Rechnung tragen. Eine Verwendung liegt daher in der eigenen Verantwortung des Lesers. Jegliche Haftung wird ausgeschlossen. Alle Rechte, auch der auszugsweisen Vervielfältigung, liegen beim Bitkom oder den jeweiligen Rechteinhabern.