New Defence: Innovationspolitische Perspektiven auf eine neue Sicherheitsarchitektur

VDI|VDE|IT

Inhalt

New Defence: Innovationspolitische Perspektiven auf eine neue Sicherheitsarchitektur

Zusammenfassung

Das vorliegende Positionspapier greift die bestehende Erweiterung sicherheitspolitischer Strategien angesichts veränderter Bedrohungslagen auf. Dabei wird der Fokus auf „New Defence" gelegt, ein innovationspolitisches Konzept, das Verteidigung als Querschnittsaufgabe neu denkt: über Ressortgrenzen hinweg, eingebettet in ein dynamisches Innovationsökosystem und verankert in der demokratischen Gesellschaft. Im Zentrum steht ein systemischer Preparedness-Ansatz, der die Fähigkeit stärkt, in Friedens-, Krisen- und Konfliktszenarien schnell, koordiniert und innovationsgetrieben zu reagieren.

Dieser Preparedness-Ansatz gliedert sich in drei miteinander verbundene Dimensionen: die militärische, die wirtschaftliche und die gesellschaftliche Preparedness.

- **Militärische Preparedness** betont die Notwendigkeit, technologische Abhängigkeiten zu reduzieren und die eigenständige Entwicklung und Integration verteidigungsrelevanter Technologien zu fördern.
- **Wirtschaftliche Preparedness** zielt auf die Stärkung kritischer Produktionskapazitäten, Lieferketten und Infrastrukturen ab, um im Krisenfall handlungsfähig zu bleiben.
- **Gesellschaftliche Preparedness** fokussiert auf die Stärkung der demokratischen Legitimation und Mitwirkung, indem die Bedingungen der gesellschaftlichen Tragfähigkeit von New Defence und deren Folgen ermittelt und berücksichtigt werden.

Ein zentrales Transformationsinstrument ist die **Förderung von Dual-Use-Technologien**. Diese Technologien bieten Lösungen für sicherheitspolitische Herausforderungen, eröffnen aber auch neue Formen der zivil-militärischen Kooperation und des Technologietransfers. Durch die systematische Integration von ziviler Forschung mit sicherheitsrelevanten Bedarfen können Deutschland und Europa Innovationskraft stärken, Abhängigkeiten reduzieren und eine umfassende Sicherheitsarchitektur aufbauen, die Schutz, Verbindung und die Stärkung demokratischer Werte vereint. New Defence ist keine Reaktion – es ist eine strategische Neuausrichtung.

Zur Umsetzung von New Defence braucht es:

- eine **strategische Forschungsförderung**, ausgerichtet an einer **Forschungs- und Innovationsstrategie** mit klarer Zielarchitektur
- einen strukturellen **Ausbau des Innovationsökosystems** einschließlich einer **Verbesserung der Rahmenbedingungen**
- neue Formate wie **Defence-Reallabore und Rapid-Prototyping-Plattformen** zur Erprobung und Beschleunigung technologischer Entwicklungen

Hintergrund – Die strategische Neudefinition der Verteidigungsfähigkeit

Nicht erst seit der Zeitenwende hat sich die sicherheitspolitische Lage Europas tiefgreifend und nachhaltig verändert. Die Rückkehr zwischenstaatlicher Gewalt, globale geopolitische Verschiebungen sowie hybride Bedrohungen in digitalen und physischen Räumen fordern eine grundlegende Neubewertung bestehender sicherheits- und verteidigungspolitischer Strategien. Klassische Abschreckung allein greift zu kurz – gefragt ist ein neues Verständnis von Sicherheit, das weit über militärische Reaktionsfähigkeit hinausgeht. Zunehmend wird deutlich: Die Resilienz europäischer Gesellschaften entscheidet sich in kritischen Infrastrukturen, digitalen Netzwerken und technologischen Wertschöpfungsketten. Energie, Kommunikation, Datenräume, Logistik – sie bilden das Rückgrat moderner Verteidigungsfähigkeit und sind zugleich hochgradig verwundbar.

In dieser veränderten Realität adressiert der Begriff **New Defence** einen paradigmatischen Perspektivwechsel: Verteidigung wird als vernetzte, strategische Querschnittsaufgabe neu definiert. Gefordert ist ein Ökosystem aus staatli-

chen Institutionen, technologiegetriebenen Unternehmen, Wissenschaft und Forschung, Start-ups, Investoren sowie zivilgesellschaftlichen Akteuren – verbunden durch eine gemeinsame Sicherheitsarchitektur mit staatlichen Streitkräften. Es gilt, auf die dynamischen Herausforderungen der neuen Sicherheitslage mit einer klaren strategischen und zugleich reflektierten Ausrichtung zu reagieren. New Defence bedeutet, technologische Innovation nicht nur im Hinblick auf Leistungsfähigkeit und Effizienz zu fördern, sondern sie als übergreifendes Zusammenspiel von Widerstandsfähigkeit, Adaptivität, Interoperabilität sowie wirtschaftlicher Einbettung und gesellschaftlicher Tragfähigkeit zu denken. Dabei nehmen Dual-Use-Technologien, interoperable Plattformen und adaptive Systeme die operative Schnittstelle zwischen militärischem Bedarf und ziviler Innovationsdynamik ein. Es geht darum, Technologien zu entwickeln und zu gestalten, die nicht nur schützen, sondern auch verbinden und Sicherheit, Freiheit und demokratische Werte in einem gemeinsamen europäischen und internationalen Rahmen stärken.

Systemische Preparedness als strategischer Handlungsrahmen

Die sicherheitspolitische Lage erfordert eine grundlegende Neuausrichtung. Weg von rein reaktiven Sicherheitskonzepten, hin zu einem proaktiven, strategisch verankerten Verständnis von Resilienz, Vorsorge und Integrationsfähigkeit. Der im Rahmen von New Defence entwickelte Preparedness-Ansatz bietet hierfür den strukturellen Handlungsrahmen. Er operationalisiert das Prinzip der Gesamtverteidigung sowie Abschreckung und adressiert die Anforderungen eines krisenfesten, technologisch souveränen und gesellschaftlich tragfähigen Deutschlands. Dieser Ansatz greift den im Jahr 2023 eingeführten Begriff der „Kriegstüchtigkeit" auf und bezieht sich auf die gesamtgesellschaftliche Handlungsfähigkeit in Friedens-, Krisen- und Konfliktphasen. Es handelt sich um einen gesamtstaatlichen Ansatz, der die Bundeswehr, aber auch andere staatliche Stellen, Unternehmen und die Gesellschaft als Ganzes einbezieht, um einen ganzheitlichen Bewusstseinswandel vorzunehmen und sich der tatsächlichen Gefahrenlage zu stellen.[1][2]

Dementsprechend setzt auch die Preparedness auf ein integratives Verständnis von Vorsorge, Fähigkeitserhalt und Innovationskraft. Der systemische Preparedness-Rahmen gliedert sich in die drei sich gegenseitig verstärkenden Dimensionen der militärischen, wirtschaftlichen und gesellschaftlichen Preparedness. Jede dieser Dimensionen eröffnet spezifische operative und inhaltliche Handlungsfelder. Zusammengenommen leisten diese einen Beitrag zu einer verlässlichen Sicherheits- und Innovationsarchitektur für ein auf allen Ebenen vorbereitetes Deutschland und Europa. Auf diese Weise ist zudem die Anschlussfähigkeit an übergeordnete Strategien wie beispielsweise den *Operationsplan Deutschland*[3], die *Nationale Sicherheitsstrategie*,[4] die *KRITIS-Strategie*[5] oder die *European Preparedness Union Strategy*[6] gewährleistet. Der Begriff Resilienz[7] hat sich in den letzten Jahren als zentrales Narrativ in Sicherheits-, Technologie- und Gesellschaftsdiskursen etabliert, stößt dabei aber zunehmend an analytische Grenzen: Seine breite Anwendung in Diskursen hat zu einer sprachlichen und konzeptionellen Verwässerung und somit zu einem unscharfen Fokus geführt.[8] In einer sicherheitspolitisch zugespitzten Lage – geprägt durch den anhaltenden russischen Angriffskrieg gegen die Ukraine, wachsendes Konfliktpotenzial im Indopazifik sowie die Zunahme hybrider Bedrohungen – reicht ein defensives Verständnis von Widerstandsfähigkeit nicht mehr aus. Was heute gefragt ist, ist nicht Reaktion, sondern eine proaktive Systemgestaltung. Dabei ist Preparedness keine militaristische Eskalationsstrategie, sondern Ausdruck einer wehrhaf-

1 Führungsakademie der Bundeswehr (2025): Gesamtverteidigung Deutschland – Ein gemeinsamer Auftrag für unsere Gesellschaft. Hamburg. Online unter https://www.bundeswehr.de/resource/blob/5961228/28fddb5850b06ba101ca692972b1f8f2/broschuere-pdf-lgan-25-ergebnispraesentation-data.pdf

2 Rahmenrichtlinien für die Gesamtverteidigung - Gesamtverteidigungsrichtlinien (RRGV) https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/sicherheit/RRGV.pdf?__blob=publicationFile&v=1

3 Presse- und Informationszentrum des Operativen Führungskommandos der Bundeswehr (2025):Operationsplan Deutschland – Eine gesamtstaatliche und gesamtgesellschaftliche Aufgabe. Berlin. Online unter https://www.bundeswehr.de/resource/blob/5920008/980d592bf03ed2e7fbb1d4a57bda712b/oplan-data.pdf

4 Presse- und Informationszentrum des Operativen Führungskommandos der Bundeswehr (2025):Operationsplan Deutschland – Eine gesamtstaatliche und gesamtgesellschaftliche Aufgabe. Berlin. Online unter https://www.bundeswehr.de/resource/blob/5920008/980d592bf03ed2e7fbb1d4a57bda712b/oplan-data.pdf

5 Bundesministerium des Inneren (2009): Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie). Berlin. Online: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/kritis.pdf?__blob=publicationFile&v=6
Aktuell (Juli 2025) befindet sich das KRITIS-Dachgesetz, das den physischen Schutz kritischer Infrastruktur erhöhen soll, in Vorbereitung.

6 European Commssion (2025): Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Council and the Committee of the Regions on the European Preparedness Union Strategy. Brussels. Online: https://webgate.ec.europa.eu/circabc-ewpp/d/d/workspace/SpacesStore/b81316ab-a513-49a1-b520-b6a6e0de6986/file.bin

7 „Resilienz beschreibt die Fähigkeit eines Systems, einer Gemeinschaft oder einer Gesellschaft, sich rechtzeitig und effizient den Auswirkungen einer Gefährdung widersetzen, diese absorbieren, sich an sie anpassen, sie umwandeln und sich von ihnen erholen zu können. Eine wichtige Voraussetzung dafür ist die Erhaltung und Wiederherstellung ihrer wesentlichen Grundstrukturen und Funktionen durch Risikomanagement." Vereinte Nationen 2016, zitiert nach Bundesamt für Bevölkerungsschutz und Katastrophenhilfe 2022 – Online: https://www.bbk.bund.de/DE/Themen/Nationale-Kontaktstelle-Sendai-Rahmenwerk/Resilienzstrategie/resilienz-strategie_node.html

8 Hanisch, Michael (2016): Was ist Resilienz? Unschärfen eines Schlüsselbegriffs. Bundesakademie für Sicherheitspolitik, Arbeitspapier Sicherheitspolitik Nr. 19/2016. Berlin. Online: https://www.baks.bund.de/sites/baks010/files/arbeitspapier_sicherheitspolitik_2016_19.pdf

ten Innovationsgesellschaft, die technologisch, organisatorisch und sozial auf dauerhafte Bedrohungslagen und tiefgreifende Schocks vorbereitet ist. Aus der Verbindung von wissenschaftlich-technologischem Wissen und systemischer Perspektive entstehen konkrete Beiträge entlang der drei Preparedness-Dimensionen.

Militärische Preparedness – Innovationspolitische Impulse für New Defence und Dual-Use

Die militärische Dimension von Preparedness stellt eine zentrale Säule der sicherheitspolitischen Neuausrichtung dar. Angesichts wachsender Bedrohungslagen und geopolitischer Spannungen gewinnt die Fähigkeit zur eigenständigen Entwicklung, industriellen Skalierung und operativen Integration verteidigungsrelevanter Technologien strategisch an Bedeutung. Trotz nominell hoher Verteidigungsausgaben von rund 425 Milliarden Euro[9] in Europa – etwa dreimal so viel wie Russlands offizielle 135 Milliarden – ergibt sich kaufkraftbereinigt eine faktische Parität. Russland erreicht inflations- und umrechnungskorrigiert rund 427 Milliarden Euro. Das stellt eine Herausforderung für die Effektivität europäischer Verteidigungsausgaben dar. Der „Draghi-Bericht" an die Europäische Kommission aus dem Jahr 2024 unterstreicht, dass 78 % der europäischen Rüstungsbeschaffung in Länder außerhalb der EU – vorzugsweise die USA – fließen, wodurch entscheidende Anteile von Wertschöpfung, strategischer Kontrolle und technologischer Souveränität ausgelagert werden.[10] Dem gegenüber stehen erhebliche Potenziale innerhalb Deutschlands. Insbesondere ist Deutschland immer noch ein global bedeutender Wissenschaftsstandort mit hoher industrieller und ökonomischer Komplexität[11], um die militärische Innovationsfähigkeit nachhaltig stärken zu können. Voraussetzung hierfür ist die konsequente Vernetzung und Förderung mit einer strategischen Perspektive.

In diesem Kontext versteht New Defence die militärische Sicherheit als integralen Bestandteil eines zivil-militärischen Innovationsraums. Die gezielte Verzahnung ziviler Forschung mit sicherheitsrelevanten Bedarfen – etwa im Bereich von Dual-Use-Technologien – bildet dabei das Rückgrat eines robusten, technologisch souveränen Verteidigungssystems; wenngleich dies in der praktischen Umsetzung weit mehr erfordert als die bloße Übertragung bestehender Technologien. Die technologische Souveränität entsteht dabei durch die systematische Bewertung, gezielte Modifikation und frühzeitige Integration ziviler Technologien mit militärischer Wirkungstiefe. Der klassische lineare Technologietransfer wird durch eine iterative Entwicklung von der Laborebene bis zur einsatznahen Erprobung ersetzt, um die Einsatzfähigkeit und Zuverlässigkeit im Gefechtsfeld sicherzustellen.

Dabei soll das Ziel verfolgt werden, verteidigungsrelevante Innovationen in kurzen Zyklen industriell skalierbar und für die Streitkräfte verfügbar zu machen. Damit wird der Innovationsprozess selbst zu einem sicherheitsstrategischen Handlungsfeld. Insbesondere der innovative Mittelstand übernimmt hier eine Schlüsselrolle. Er liefert kritische Komponenten, sorgt für kontinuierliche Forschung und wirkt als Impulsgeber für das gesamte sicherheitsrelevante Technologiesystem. Um die vielfältigen militärischen Fähigkeiten realisieren zu können, benötigen die Streitkräfte umfassend integrierte Waffensysteme. Die auf bestimmte Einsatzbereiche festgelegten großen Rüstungskonzerne sind dabei auf die spezialisierten Produkte eines innovativen Mittelstands angewiesen, der essenzielle Komponenten liefert und durch kontinuierliche Forschung und Entwicklung die Innovationskraft der gesamten Branche stärkt. Die Wettbewerbsfähigkeit des Sektors hängt somit maßgeblich auch von der Leistungsfähigkeit des Mittelstands ab.[12] Gleichzeitig bestehen weiterhin strukturelle Abhängigkeiten. Als Beispiel sind Drohnenkomponenten aus China zu nennen, wie Batterien, Motoren, Magnete, elektronische Steuerungen, Kameras und Propeller. Diese strategischen Schwachstellen unterstrei-

9 International Institute for Strategic Studies (2025): The Military Balance 2025. London.

10 Draghi, Mario (ed.) (2024). The Draghi report: A competitiveness strategy for Europe. European Commission, Brussels, p. 60. Online: https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en?filename=The%20future%20of%20European%20competitiveness%20_%20A%20competitiveness%20strategy%20for%20Europe.pdf

11 Hidalgo, César A.; Hausmann, Ricardo (2009): The building blocks of economic complexity. PNAS, vol. 106 (26), p. 10570-10575. Online: https://doi.org/10.1073/pnas.0900943106

12 Niclas, Marc (2025): Rüstungsindustrie: Kapitalmangel gefährdet Verteidigungsfähigkeit. ‚Standpunkt' im Security.Table vom 23.07.2025.

chen die Notwendigkeit gezielter Reindustrialisierung und Technologieautonomie.

Als Zielbild der militärischen Preparedness entwickelt sich Deutschland zu einem international wettbewerbsfähigen Innovationsstandort im Bereich New Defence und Dual-Use. Auf Basis wissenschaftlicher Exzellenz, industrieller Breite und hoher ökonomischer Komplexität kann ein zivil-militärisches Forschungs- und Entwicklungsökosystem entstehen, das technologiesouveräne Lösungen mit sicherheitspolitischem Mehrwert hervorbringt. Dies erfordert systemisches Handeln, organisatorische Lernfähigkeit und strategisch koordinierte Innovationsprozesse.

Militärische Preparedness verlangt nach der gezielten Förderung sicherheitsrelevanter Innovationen entlang des gesamten technologischen Entwicklungspfads von der Grundlagenforschung über die Anwendung bis hin zur operativen Integration. Entscheidend ist die Etablierung eines innovationspolitischen Rahmens, der das Zusammenspiel zwischen staatlicher Bedarfssteuerung und Beschaffung, wirtschaftlicher Dynamik und wissenschaftlicher Exzellenz nachhaltig fördert. Ein integrativer Bestandteil dieser Rahmensetzung ist die strukturelle Verankerung von Dual-Use-Innovationen in der Hightech-Agenda der Bundesregierung. Relevante Signale sind in den bekannt gewordenen Entwürfen zum kommenden 10. Europäischen Forschungsrahmenprogramm (FP)[13] und zum European Competitiveness Fund (ECF)[14] sichtbar. Ab dem Jahr 2028 soll eines der vier als „Policy Windows" bezeichneten strategischen Felder den (Arbeits-) Titel „Resilience, Defence & Space" tragen.

Die konsequente Verknüpfung des zivilen und militärischen Innovationsökosystems, ist kein Sonderweg, sondern Ausdruck eines strategischen Grundverständnisses: Sicherheit, technologische Leistungsfähigkeit und gesellschaftliche Innovationskraft sind systemisch miteinander verbunden. Zukunftsfähigkeit entsteht, wo ressortübergreifendes Denken, technologieoffene Förderung und systematische Vermittlung zwischen Friedensnutzung und Krisenfestigkeit zusammenkommen. Schlüsselbereiche mit Dual-Use-Potenzial weisen nicht nur eine hohe sicherheitspolitische Bedeutung auf, sondern ermöglichen auch zivilgesellschaftlichen und wirtschaftlichen Mehrwert. Innovationspolitische Rahmensetzungen und Roadmaps helfen als strukturierende Instrumente dabei, den doppelten Nutzen sichtbar, steuer- und nutzbar zu machen sowie langfristige Ziele und Umsetzungsschritte anhand benötigter Fähigkeiten zu formulieren. Ein Hochtechnologieansatz kann sich beispielsweise aus der systemischen Ähnlichkeit von Software-defined Warfare[15] (inkl. einer Combat Cloud) auf der militärischen und Software-defined Vehicle[16] (inkl. Car-to-X) auf der zivilen Seite ergeben, sodass es sinnvoll sein kann, Important Projects of Common European Interest (IPCEI) für den Dual-Use-Bereich zu definieren. Zu dieser zivil-militärischen Strategieentwicklung gehört eine Erweiterung der kontinuierlichen Bewertung disruptiver Technologien im Verteidigungskontext. Die Bewertung schließt die frühzeitige Normung, Zertifizierung und Testverfahren ein, um regulatorische Hürden zu minimieren und Skalierung zu ermöglichen. Auch dies betont der „Draghi-Bericht" an die Europäische Kommission in Hinblick auf die technologische Souveränität Europas.[17]

Der Aufbau sicherer und interoperabler Innovationskorridore – mit Institutionen wie der Bundeswehr und ihrem Cyber Innovation Hub, dem Bundesamt für Sicherheit in der Informationstechnik (BSI), dem Deutschen Institut für Normung (DIN), der European Defence Agency (EDA), der NATO mit ihrem Innovation Fund (NIF) sowie zivilen Partnern – ermöglicht es, technologische Entwicklungen effizient in bestehende sicherheitsrelevante Architekturen zu integrieren. Ein weiterer strategischer Hebel ist der Technologietransfer durch gezielte Förderung verteidigungsnaher Start-ups. Besonders Deep-Tech-Gründungen verfügen über das Potenzial, sicherheitsrelevante Disruptionen hervorzubringen. Dazu bedarf es verteidigungsbezogener Innovationsprogramme, die auf Dual-Use und spezifische

13 European Commission (2025): Proposal for a Regulation of the European Parliament and the Council establishing Horizon Europe, the Framework Programme for Research and Innovation, for the period 2028-2034 laying down its rules for participation and dissemination, and repealing Regulation (EU) 2021/695. Brussels. Online: https://sciencebusiness.net/sites/default/files/inline-files/HE-FP10%20-%20draft%20regulation.pdf

14 European Commission (2025): Proposal for a Regulation of the European Parliament and the Council establishing the European Competitiveness Fund (‚ECF)', including the specific programme for defence research and innovation activities, and repealing Regulations (EU) 2021/522, (EU) 2021/694, (EU) 2021/696, (EU) 2021/697, (EU) 2021/783, (EU) 2023/588, (EU) 2023/1525, (EU) 2023/2418, (EU) [EDIP. Brussels. Online: https://www.euractiv.com/wp-content/uploads/sites/2/2025/07/Euractiv-2.pdf

15 Mulchandadi, Nand; Shanahan, John N.T. (2022): Software-defined Warfare: Architecting the DOD's Transition to the Digital Age. Center for Strategic & International Studies, CSIS Strategic Technologies Program. Washington, DC. Online: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/220907-Mulchandani-SoftwareDefined-Warfare.pdf?VersionId=ZH_PqTS4JKch4dOfcHT35kzC2WqnZKnV

16 European Commission (2023): Concept paper on an open European software-defined vehicle platform for the vehicle of the future. Prepared by Directorate-General for Communications Networks, Content and Technology, with support by McKinsey & Company. Brussels. Online: https://ec.europa.eu/newsroom/dae/redirection/document/96183

17 Draghi, Mario (ed.) (2024). The Draghi report: A competitiveness strategy for Europe. European Commission, Brussels. Online: https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en?filename=The%20future%20of%20European%20competitiveness%20_%20A%20competitiveness%20strategy%20for%20Europe.pdf

Innovations-Hubs für Start-ups im Bereich New Defence ausgerichtet sind.

Im Fokus sollten dabei insbesondere Technologien mit hohem strategischem Hebel stehen, so etwa in den Bereichen Sensorik, Raumfahrt, Künstliche Intelligenz, Quantentechnologien, Cybersicherheit, Robotik, Materialwissenschaften, Additive Fertigung, oder Energieversorgung. Ziel ist es, Innovationsdynamiken gezielt in jene Bereiche zu lenken, die sowohl für die zivile Wettbewerbsfähigkeit als auch für die militärische Preparedness zentral sind. Ziel ist es, bislang ungenutzte Innovationspotenziale durch neue Anreizsysteme zu mobilisieren. Die Anreizsysteme schließen flexiblere Vergabeverfahren oder strategische Kooperationsformate mit europäischen Partnern ein. Dazu bedarf es auch belastbarer Transferformate zwischen Wissenschaft, Industrie und sicherheitsrelevanten Bedarfsträgern. Transferformate wie Matching-Plattformen, skalierbare Inkubatoren und agile Testfelder helfen, Technologien frühzeitig zu identifizieren, an militärische Anforderungen anzupassen und zur Marktreife zu führen. Besonders wirkungsvoll ist dieser Ansatz dann, wenn er technologieoffen ausgestaltet und zugleich durch ein agiles Management unterstützt wird, das den Austausch zwischen allen Akteuren aktiv moderiert. Flankierend hierzu sollten Monitoring- und Evaluationsformate etabliert werden, die verteidigungsrelevante Technologieentwicklungen mess- und steuerbar machen. Dies betrifft sowohl die Identifikation strategischer Technologiefelder, als auch die Analyse von Abhängigkeiten, Entwicklungsständen und internationaler Wettbewerbslagen. Ziel ist ein präzises Bild der militärischen Preparedness Deutschlands, das sowohl die operative Innovationsförderung, als auch die langfristige Fähigkeitsplanung fundiert unterstützt.

Zusammenfassend betont die Nationale Sicherheitsstrategie die Notwendigkeit eines wehrhaften Staates und moderner Streitkräfte. Der militärische Innovationsraum muss daher als strategisches Technologiefeld betrachtet werden. Dual-Use-Potenziale, Start-up-Innovationen und Hochtechnologien müssen beschleunigt in die Fähigkeitsplanung der Bundeswehr überführt werden. Eine strukturierte Projektförderung entlang operationeller Prioritäten kann diese Übersetzung von Forschung in militärische Wirkung systematisch unterstützen:

- Entwicklung eines ressortübergreifenden Innovationsprogramms „New Defence“
- Einrichtung verteidigungsnaher Innovations-Hubs mit Fokus auf Start-ups und Deep-Tech
- Auf Dual Use ausgerichtete Umsetzung der sicherheitsrelevanten Technologiefelder (KI, Sensorik, Robotik, Cyber) in der Hightech-Agenda der Bundesregierung
- Etablierung agiler Projektlinien zur schnellen Erprobung und Skalierung von Dual-Use-Technologien
- Förderung von Technologietransfer zwischen zivilen Forschungsakteuren und Bundeswehrstrukturen

Wirtschaftliche Preparedness – Souveräne Produktions- und Versorgungskapazitäten

Die wirtschaftliche Dimension von Preparedness zielt auf die Fähigkeit eines Landes, im Krisen- oder Konfliktfall wirtschaftlich handlungsfähig zu bleiben, kritische Lieferketten zu stabilisieren und zentrale Produktionsprozesse flexibel zu skalieren. Deutschland besitzt als hochvernetzte, technologisch entwickelte Volkswirtschaft grundsätzlich die Voraussetzungen, diese Aufgaben zu erfüllen. Dennoch müssen strategische Verwundbarkeiten frühzeitig erkannt und systematisch adressiert werden. Wirtschaftliche Kriegstüchtigkeit bedeutet in diesem Kontext nicht die Militarisierung der Ökonomie, sondern die gezielte Befähigung zur Resilienz, Mobilisierung und Systemadaption in sicherheitskritischen Szenarien.

> *Als Zielbild der wirtschaftlichen Preparedness ist die deutsche Volkswirtschaft im Ernstfall in der Lage, essenzielle Funktionsfähigkeiten sicherzustellen und Engpässe zu kompensieren, indem die zentrale Produktion, kritische Infrastrukturen und logistische Knotenpunkte aufrechterhalten bzw. zeitnah wiederhergestellt werden. Im Fokus stehen flexible Allokationsmechanismen, die kritische Ressourcen und Produktionsprozesse auf sicherheitsrelevante Prioritäten ausrichten.*

Im Zentrum einer wirtschaftlichen Preparedness steht die Identifikation und systematische Stärkung kritischer Pro-

duktionsinfrastrukturen. Hierzu zählt die gezielte Förderung von Schlüsselindustrien wie der Herstellung von Munition, Ersatzteilen, Schutzsystemen, Treibstoffen sowie essenzieller pharmazeutischer Produkte. Diese Industrien bilden das Rückgrat einer funktionalen Sicherheitsvorsorge und müssen in Friedenszeiten durch Investitionen, Innovationsimpulse und Regulierungsanpassungen abgesichert und ertüchtigt werden. Gleichzeitig ist die Widerstandsfähigkeit kritischer Infrastrukturen entlang der gesamten zivilen Versorgungskette, wie Energie, Wasser, Lebensmittel, Gesundheit, Kommunikation, Entsorgung und Logistik, ein zentraler Hebel wirtschaftlicher Preparedness. Erforderlich sind technologiegetriebene Modernisierungen, als auch organisatorische und finanzielle Modelle, die eine flexible Reaktivierung, Notfallversorgung oder systemische Skalierung ermöglichen. Ergänzend zur Forschung und Innovationsförderung sind hier Investitionsprogramme notwendig, die wirtschaftliche Robustheit im Sinne sicherheitsstrategischer Resilienz ermöglichen. Die Aussage des Bundesverteidigungsministers im Juli 2025, dass es keinen Grund mehr für die deutsche Rüstungsindustrie gebe, Produktionskapazitäten nicht auszuweiten,[18] verdeutlicht den Handlungsdruck, neue Formen der zivil-militärischen Kooperationsarchitektur zu schaffen. Ein Beispiel dafür ist der Förderaufruf der Invest BW Innovationsförderung vom Mai 2025, der unter anderem gezielt Dual-Use-Innovationen im Themenbereich „Maschinenbau, Robotik und Verteidigung adressiert".[19]

Angesichts zunehmender geopolitischer Unsicherheiten gewinnt die Rückverlagerung sicherheitskritischer Produktionskapazitäten, sogenanntes Reshoring oder Nearshoring, stark an Bedeutung. Die Abhängigkeit von wenigen außereuropäischen Herstellern bei der Chipfertigung, pharmazeutischen Grundstoffen oder Softwarearchitekturen stellt ein strategisches Risiko dar. Eine wirtschaftliche Preparedness-Strategie muss daher auf eine Diversifikation, Redundanz und europäische Wertschöpfungstiefe ausgerichtet sein. Der Bereich Logistik wird dabei zum operationellen Rückgrat wirtschaftlicher Verteidigungsfähigkeit. Kritische Verkehrskorridore, multimodale Logistik-Hubs und transnationale Versorgungslinien sind gezielt zu identifizieren, abzusichern und krisenfest auszubauen, um insbesondere militärische und humanitäre Transporte im europäischen Raum durchführen zu können.

Darüber hinaus ist eine vorausschauende Personalstrategie für sicherheitsrelevante Branchen unerlässlich. Der Ausbau von Weiterbildungs- und Qualifizierungsformaten in Bereichen wie Cybersicherheit, Krisenlogistik, Versorgungstechnologie und resilienter Kommunikation ist entscheidend. Ausbildungsinhalte sollten dabei nicht nur technisches Fachwissen vermitteln, sondern auch grundlegende Kenntnisse in Sicherheitslogik, Risikoabschätzung und zivil-militärischer Kooperation, um so selbstverständlicher Teil der betrieblichen Praxis zu werden. Die Sicherung von Know-how, Dateninfrastrukturen und geschäftskritischem Wissen wird zur Voraussetzung für unternehmerische Resilienz. Unternehmen, die bereit sind, ihre Fertigung im Krisenfall gesamtstaatlich bereitzustellen, benötigen spezifische Schutzmechanismen gegen Sabotage, Spionage und Desinformationskampagnen. Ein zentraler Hebel ist hier die verbindliche Umsetzung der europäischen NIS-2-Sicherheitsrichtlinie, die rund 29.000 Unternehmen in Deutschland betrifft. Darunter sind vor allem größere Unternehmen aus den Sektoren Energie, Verkehr, Trinkwasser, Lebensmittelproduktion, Abwasser und Telekommunikation.[20]

Zusätzliche Robustheit kann durch den Aufbau eines vertraulichen, bundesweiten Registers mobilisierbarer Produktionsanlagen entstehen. Dieses auf Freiwilligkeit basierende Register sollte datenbasiert Informationen zu Kapazitäten, Umrüstoptionen und logistischen Schnittstellen bündeln – mit aktiver Einbindung von Ländern und Kommunen, insbesondere bei der Integration wirtschaftlicher Vorsorge in Katastrophenschutzpläne und bei der Identifikation regionaler Versorgungsrisiken. Ziel ist eine bessere Integration wirtschaftlicher Resilienzmaßnahmen in Katastrophenschutzpläne und regionale Risikobewertungen.

Resultierend sind Wirtschaftsmodelle für den Krisen- und Konfliktmodus erforderlich, die es ermöglichen, die Produktion und Güterversorgung je nach Bedrohungs- und Bedürfnislage und Fachkräfteverfügbarkeit zu gewährleisten. Insbesondere gilt es, systemisch relevante Akteure zu identifizieren, Interdependenzen zwischen zivilen und militärischen Bedarfsträgern zu kartieren und verlässliche Indikatoren für die Reaktionsfähigkeit ganzer Wertschöpfungsketten zu entwickeln. Mit der Modellierung von Mobilisierungsökonomien müssen nicht nur ökonomische Faktoren wie Produktionsverlagerung, dynamische Ressourcenallokation und Versorgungsengpässe prospektiv analysiert werden, sondern auch gesellschaftliche Auswirkungen etwa in Form der Arbeitskräfteverfügbarkeit

18 Pitel, Laura; Chassany, Anne-Sylvaine (2025): German Defence Minister calls on Arms Makers to deliver. Financial Times, published 13.07.2025. Online: https://www.ft.com/content/a9c8d754-bea4-4f5a-887c-b2898b5d0dd3

19 Ministerium für Wirtschaft, Arbeit und Tourismus Baden-Württemberg (2025): Invest BW Innovationsförderung – Erster Förderaufruf der 4. Phase vom 8. Mai 2025. Stuttgart. Online: https://invest-bw.de/wp-content/uploads/2025/05/20250508-Foerderaufruf-Invest-BW-IV-1-Foerderaufruf-barrierefrei.pdf

20 Heise online (2025): BSI-Chefin: Cyberschutz-Verpflichtung für Firmen ab 2026. Meldung vom 12.07.2025. Online: https://www.heise.de/news/BSI-bietet-Hilfe-bei-NIS2-an-Gesetz-soll-2026-greifen-10485024.html

und des Erhalts sozialer Infrastruktur. Ziel ist ein realitätsnahes Lagebild, das im Falle eskalierender Konflikte oder systemischer Störungen als Grundlage für politische Entscheidungen dient.

Zusammenfassend müssen krisenkritische Produktions-, Logistik- und Versorgungskapazitäten strategisch identifiziert, geschützt und gezielt entwickelt werden. Die Hightech-Agenda bietet hierfür den Rahmen, der durch sicherheitsorientierte Förderlinien und industriepolitische Impulse ergänzt werden muss – im Sinne einer aktiven wirtschaftlichen Vorsorgepolitik:

- Aufbau eines nationalen Lagebilds kritischer Wirtschaftsstrukturen mit Mobilisierungspotenzial
- Förderung sicherheitsrelevanter Produktions- und Logistikkapazitäten in Industrie und Mittelstand
- Resilienzkomponenten in industriepolitischen Förderprogrammen strukturell verankern
- Etablierung von Qualifizierungsprogrammen zu Sicherheit und Krisenvorsorge in Schlüsselbranchen
- Entwicklung steuerlicher oder regulatorischer Anreizsysteme für Unternehmen, sich an nationaler Preparedness zu beteiligen

Gesellschaftliche Preparedness – Rückhalt, Widerstandsfähigkeit, Legitimität

Gesellschaftliche Preparedness beschreibt die kollektive Befähigung einer offenen, demokratischen Gesellschaft, sicherheitspolitische Herausforderungen nicht nur zu bewältigen, sondern aktiv mitzutragen und dies, ohne dabei ihre pluralistische Struktur, institutionelle Funktionsfähigkeit und ihre normative Stabilität zu verlieren. Sie geht deutlich über temporäre Solidaritätsbekundungen hinaus. Gemeint ist ein informiertes, partizipatives Gemeinwesen, das Sicherheit als gesamtgesellschaftliche Aufgabe versteht und Verantwortung zwischen Staat, Wirtschaft, Zivilgesellschaft und Individuen strategisch teilt.

> *Als Zielbild der gesellschaftlichen Preparedness ist Deutschland eine auch im Krisen- und Konfliktfall offene, pluralistische Gesellschaft, die auch unter Krisenbedingungen handlungsfähig bleibt, ihre demokratischen Grundwerte verteidigt und gesellschaftliche Belastungen solidarisch ausbalanciert. Dabei geht es nicht um Militarisierung im Inneren, sondern um die Integration der Gesellschaft in gesamtstaatliche Sicherheitsarchitekturen, mit dem Ziel, kollektive Reaktions- und Anpassungsfähigkeit wirksam zu entfalten.*

Die Grundlage bilden die vier Säulen der Zivilen Verteidigung: die Aufrechterhaltung der Staats- und Regierungsfunktionen, der Zivilschutz, die Versorgung der Bevölkerung sowie die Unterstützung der Streitkräfte.[21] Dabei sind vor allem die Mobilisierbarkeit ehrenamtlicher Ressourcen, die Einbindung und die systematische Erhöhung zivilgesellschaftlicher Durchhaltefähigkeit die wesentlichen Erfolgsfaktoren im Krisenfall.

Ein strategischer Hebel ist der Aufbau einer faktenbasierten, vertrauensbildenden Kommunikationsarchitektur. Sicherheit muss nicht als Bedrohungsnarrativ, sondern als Ausdruck kollektiver Handlungsfähigkeit vermittelt werden. Erfolgsentscheidend ist dabei die narrative Verknüpfung von Verteidigungsfähigkeit, technologischer Innovation und gesellschaftlichem Zusammenhalt. Partizipative Formate und positive Zukunftsbilder stärken den Zusammenhalt, fördern Vertrauen und schaffen Anschlussfähigkeit an politische Entscheidungsprozesse. Gesellschaftliche Preparedness im Sinne der Gesamtverteidigung sollte daher als langfristige Gemeinschaftsaufgabe begriffen werden, bei der Bürgerinnen und Bürger, Bildungseinrichtungen, Medien, Unternehmen und der Staat gemeinsam Verantwortung übernehmen. Der Aufbau eines robusten gesellschaftlichen Sicherheitsbewusstseins, das auf Aufklärung, Beteiligung und Selbstwirksamkeit basiert, kann wesentlich zur Funktionsfähigkeit demokratischer Systeme unter Stress beitragen.

21 Bundesministerium des Inneren (2016): Konzeption Zivile Verteidigung. Berlin. Online: https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/bevoelkerungsschutz/konzeption-zivile-verteidigung.html

Ein weiterer zentraler Hebel liegt in der gezielten Förderung zivilgesellschaftlicher Sicherheitsinitiativen. Projekte, die Bildung, bürgerschaftliches Engagement und Strukturbildung verbinden, tragen zur Stärkung des gesellschaftlichen Zusammenhalts bei. Besonders relevant ist dies im Bereich der Informationssicherheit: Die Abwehr von Desinformationskampagnen erfordert nicht nur technische Kapazitäten und Medienkompetenz, sondern auch ein gesellschaftlich verankertes, vertrauenswürdiges Kommunikationsökosystem. Nur wenn staatliche Stellen, Medien, Wissenschaft und Zivilgesellschaft koordiniert handeln, kann die Bevölkerung auch in sensiblen Lagen flächendeckend, glaubwürdig und differenziert informiert werden. Ein ausbaufähiger Baustein der gesellschaftlichen Preparedness ist die strukturierte Einbindung der Bevölkerung in die Krisenvorsorge. Modelle wie eine verpflichtende oder freiwillige Dienstverpflichtung im Zivilschutz, Notfalltrainings für Haushalte oder breit angelegte Vorsorgekampagnen mit klaren Selbstschutzempfehlungen könnten dazu beitragen, ein grundlegendes Sicherheitsbewusstsein in der Bevölkerung zu verankern.[22]

Insbesondere in Ballungsräumen kommt der Stärkung der Infrastrukturresilienz eine zentrale Bedeutung zu. Der gezielte Ausbau von Schutzräumen, autarken Versorgungsmodulen und digitalen Frühwarnsystemen trägt maßgeblich dazu bei, die Widerstandsfähigkeit urbaner Räume zu erhöhen. Solche Maßnahmen sind keine abstrakte Vorsorge, sondern ein konkreter und messbarer Ausdruck gesellschaftlicher Handlungsfähigkeit angesichts zunehmender Unsicherheiten.

Die Integration sicherheitstechnischer Fragestellungen in MINT-Fächer, die Nutzung partizipativer Formate wie Citizen Science in Frühwarnsystemen oder Awareness-Programme zur Förderung digitaler Resilienz schaffen Anknüpfungspunkte für junge Menschen und binden sie frühzeitig in sicherheitsrelevante Debatten ein. Solche Formate stärken nicht nur die Anschlussfähigkeit an sicherheitspolitische Diskurse, sondern fördern auch die Selbstwirksamkeit und Verantwortungsbereitschaft der Bürgerinnen und Bürger als zentrale Ressourcen für gesellschaftliche Preparedness.

Ein umfassendes Verständnis der gesellschaftlichen Preparedness schließt dabei auch eine krisenfeste, ethisch reflektierte Gesundheitsversorgung ein. Dies umfasst die medizinische Versorgung von Zivilbevölkerung und Militärpersonen im Krisenfall. Neben der materiellen Ausstattung (etwa in Bezug auf Notfallreserven oder medizinische Logistik) geht es hier um die Vorbereitung auf ethisch komplexe Entscheidungen unter Ressourcenknappheit, wie sie etwa im Rahmen einer Triage auftreten können. Denn: „Eine NATO-Simulation geht davon aus, dass – falls Deutschland nicht nur Aufmarschgebiet, sondern auch Verwundetendrehscheibe würde – täglich mit etwa 1.000 Patientinnen und Patienten zu rechnen ist.“[23] Erforderlich sind transparente Kriterien, nachvollziehbare Entscheidungsprozesse und eine breite gesellschaftliche Debatte über Legitimation und Zumutbarkeit medizinischer Priorisierungen im Ernstfall. Nur durch eine solche Vorbereitung lässt sich Vertrauen in das Gesundheitssystem auch in extremen Belastungslagen erhalten.

Gesellschaftliche Preparedness muss dabei immer im Spannungsfeld zwischen individueller Freiheit, staatlicher Fürsorgepflicht und gemeinschaftlicher Verantwortung reflektiert werden. Eine breite Debatte über Grundhaltungen in Ausnahmesituationen, etwa zur Eigenverantwortung, Solidarität oder zum Verhältnis von Sicherheit und Freiheit, kann dabei helfen, normative Klarheit und gesellschaftliche Resilienz zu schaffen. Um die Wirkung solcher Strategien vorausschauend abzusichern, braucht es analytische Instrumente: Wirkungsanalysen, Szenarien der Strategischen Vorausschau und Studien zu demokratischer Belastbarkeit und sozialer Kohärenz unter Stressbedingungen sind hierfür essenziell. Diese sollten interdisziplinär, empirisch belastbar und normativ sensibel sein, indem sie beispielsweise Zielkonflikte zwischen Freiheit, Sicherheit und Solidarität reflektieren und zur politischen Entscheidungsfähigkeit in Krisensituationen beitragen. Auf diese Weise kann gesellschaftliche Preparedness als Frühwarnindikator wirken, mögliche Kipppunkte identifizieren und Rückwirkungen auf die wirtschaftliche oder militärische Preparedness frühzeitig sichtbar machen.

Insgesamt bedarf es eines ressortübergreifenden nationalen Leitbildes gesellschaftlicher Preparedness, das Prinzipien, Zuständigkeiten und Zielbilder klar beschreibt. Eine solche Rahmensetzung kann Orientierung geben, Maßnahmen bündeln und die Akteursvielfalt strategisch koordinieren. Gesellschaftliche Preparedness muss somit als dynamischer, lernfähiger Prozess verstanden werden. Wissenschaftlich fundierte Studien, indikatorenbasierte Monitoringinstrumente und kontinuierliche Vorausschau tragen dazu bei, diesen Prozess nicht nur analytisch zu begleiten, sondern auch operativ zu gestalten. Auf diese Weise wird die Basis gelegt für eine inklusive, antizipierende Governance als integraler Bestandteil einer in die Zukunft gerichteten Sicherheitsarchitektur, die Sicherheit

22 Egleder, Julia (2024): Zivile Verteidigung: Wie Schweden und Finnland ihre Bürger schützen. Verband der Reservisten der Deutschen Bundeswehr e. V. online vom 28.07.2025. Online: https://www.reservistenverband.de/magazin-loyal/zivile-verteidigung-schweden-finnland/

23 Frank, Matthias (2025): Auftaktveranstaltung ‘Symposium Gesundheitsversorgung in der Landesverteidigung‘. Bundeswehr online vom 02.06.2025. Online: https://www.bundeswehr.de/de/organisation/unterstuetzungsbereich/meldungen/symposium-gesundheitsversorgung-landesverteidigung-5951184

nicht als Reaktion auf Bedrohung, sondern als proaktive Gestaltung komplexer Zukunftsrisiken begreift.

Zusammenfassend beginnt die gesellschaftliche Preparedness mit Information, Bildung und Einbindung. Bürgerinnen und Bürger müssen vorbereitet, beteiligt und befähigt werden, um im Krisenfall handlungsfähig zu bleiben. Dafür braucht es verbindliche Programme zur Sicherheitsbildung, einen modernen Zivilschutz und ein krisenfähiges Kommunikationsökosystem. Die Nationale Sicherheitsstrategie fordert zu Recht eine Sicherheitsarchitektur „aus der Mitte der Gesellschaft" – diese muss jetzt operativ umgesetzt werden:

- Entwicklung eines ressortübergreifenden Leitbilds „Gesellschaftliche Preparedness"
- Förderung partizipativer Sicherheitsformate (z. B. Citizen Science, Notfalltrainings, Krisenplanspiele)
- Systematische Einbindung von Zivilschutz- und Katastrophenschutzthemen in Bildungs- und MINT-Programme
- Auflage eines Programms „Digitale Prepardness & Krisenkommunikation" mit Fokus auf Medienbildung und Infrastruktur
- Schaffung bzw. Förderung resilienter Schutz- und Versorgungsstrukturen insbesondere in urbanen Räumen (z. B. Schutzräume, autarke Module)

Call for Action

Das vorliegende Positionspapier verdeutlicht die Notwendigkeit einer umfassenden Neuausrichtung unserer Sicherheitsarchitektur auf Basis von Forschung, Entwicklung und Innovation. Im Mittelpunkt einer raschen Verwirklichung der drei skizzierten Zielbilder für die militärische, wirtschaftliche und gesellschaftliche Preparedness stehen aus Sicht der VDI/VDE-IT die folgenden Handlungsfelder und Maßnahmen:

1. Strategische Forschungsförderung:

- Fokus Dual-Use-Technologien: Erhöhung der Fördermittel für Forschungsprojekte mit klarem Dual-Use-Potenzial in Bereichen wie KI, Quantentechnologien, Robotik, Cybersicherheit und Sensorik, sowie Unterstützung beim Aufbau zivil-militärischer Produktionskapazitäten
- Thematische Schwerpunkte: Ausweisung von Förderschwerpunkten entlang der drei Preparedness-Dimensionen (militärisch, wirtschaftlich, gesellschaftlich) mit klaren Innovationszielen
- Langfristige Perspektiven: Schaffung von Rahmenbedingungen für langfristige, risikoreiche und kapitalintensive Forschungsprojekte, die über traditionelle Projektlaufzeiten hinausgehen

2. Innovationsökosystem stärken:

- **Gründungsförderung**: Etablierung spezialisierter Förderprogramme für Deep-Tech-Start-ups im Bereich Verteidigung und Sicherheit, inklusive Inkubatoren und Acceleratoren
- **Technologietransfer**: Förderung des Transfers von Forschungsergebnissen in die industrielle Anwendung durch gezielte Programme und Kooperationen zwischen Forschungseinrichtungen, Unternehmen und Bundeswehr
- **Test- und Erprobungsräume**: Ausbau und Vernetzung von Test- und Erprobungszentren für innovative Sicherheitstechnologien, die einen schnellen Innovationszyklus ermöglichen
- **Unterstützung für KMU verbessern**: Der Zugang von kleinen und mittelständischen Unternehmen (KMU) der zivilen Wirtschaft zu sicherheitsrelevanten Informationen und Unterstützungsangeboten muss erweitert und vereinfacht werden

3. Rahmenbedingungen verbessern:

- **Vereinfachte Vergabeverfahren**: Schaffung flexibler und schneller Vergabeverfahren für sicherheitsrelevante Technologien, die KMU den Zugang zum Markt erleichtern
- **Standardisierung & Zertifizierung**: Förderung der Standardisierung und Zertifizierung von Schlüsseltechnologien, um Interoperabilität und Vertrauen zu gewährleisten
- **Internationale Kooperation**: Stärkung der europäischen Zusammenarbeit in Forschung und Innovation im Bereich Verteidigung, insbesondere im Rahmen des European Defence Fund (EDF)

4. Kompetenzaufbau:

- **Ausbildungsoffensive**: Förderung von Studiengängen und Weiterbildungsangeboten im Bereich Sicherheitstechnologien, um den Fachkräftebedarf zu decken
- **Interdisziplinäre Zusammenarbeit**: Förderung der Zusammenarbeit zwischen Ingenieurwissenschaften, Informatik, Sozialwissenschaften und anderen relevanten Disziplinen
- **Zivilklausel**: Klärung des Umgangs mit Zivilklauseln an Hochschulen bzw. Ermöglichung von Ausnahmen

Eine Umsetzung dieser Maßnahmen kann die Innovationskraft Deutschlands und Europas im Bereich Sicherheit stärken, die Souveränität gewährleisten und das Funktionieren einer demokratisch verfassten, pluralistischen und handlungsfähigen Gesellschaft sicherstellen. In einer konzertierten Aktion unter ausdrücklichem Einschluss der Zivilgesellschaft in ihrer Vielfalt können die Herausforderungen einer „New Defence" erfolgreich bewältigt und eine multidimensionale Preparedness erreicht werden.

Autoren

Michael Preuß-Eisele ist Leiter der Gruppe Skalierbare Lösungen für Förderprogramme innerhalb der Abteilung Forschung und Entwicklung. Schwerpunkt seiner Arbeit ist es, die Innovationspotenziale in der VDI/VDE-IT auszuschöpfen und die digitale Transformation des Unternehmens zu befördern. Darüber hinaus ist er Experte für verteidigungs- und rüstungsrelevante Themen. Als Kapitänleutnant hat er unter anderem die szenariobasierte Beschaffung von Ausrüstung und deren Nutzung für das Planungsamt der Bundeswehr weiterentwickelt.

Eric Hustig engagiert sich im Rahmen seiner ehrenamtlichen Tätigkeit beim Technischen Hilfswerk (THW) aktiv für den Bevölkerungsschutz. Bei der VDI/VDE-IT ist er Qualitäts- und Prozessbeauftragter im Bereich Administratives Projektmanagement. Dort fokussiert er sich besonders auf die Weiterentwicklung der administrativen Prozesse und die Einführung neuer Ideen in den Arbeitsalltag.

Roland Krebs ist Berater für Künstliche Intelligenz im Bereich Technologien des digitalen Wandels bei der VDI/VDE-IT. Der Schwerpunkt seiner Arbeit liegt dabei auf Data Science, Kommunikationstechnologien, IT-Sicherheitstechnologien und elektronischen Systemen. Er war zuvor für das Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw) als Berater für Sensortechnologien sowie als Project Officer Radio Frequency Sensor Technologies bei der European Defence Agency (EDA) tätig.

Marc Bovenschulte ist Leiter des Bereichs Demografie, Cluster und Zukunftsforschung. Seine Schwerpunkte sind die strategische Vorausschau, die Auswirkungen von Transformationsprozessen sowie die Schnittfläche aus Geo- und Technologiepolitik. Hier liegt das Augenmerk auf der Kompensation einseitiger Abhängigkeiten zur Stärkung der technologischen und wirtschaftlichen Souveränität.

Herausgegeber:
VDI/VDE Innovation + Technik GmbH
Steinplatz 1 | 10623 Berlin
www.vdivde-it.de

Bildnachweis:
Adobe Stock/Nataliya Hora/Christian Schwier/filmbildfabrik

© VDI/VDE-IT 2025