bwconsulting

Comprehensive Defence

Sicherheit als gesamtstaatliche und gesamtgesellschaftliche Aufgabe

Gesamtstaatliche und gesamtgesellschaftliche Verteidigung

Der russische Angriffskrieg gegen die Ukraine hat eine neue Ära für Deutschland und Europa eingeleitet. Bündnisse verändern sich, langjährige Partner ziehen sich zurück. Sicherheit ist etwas, für das Europa wieder selbst stärker einstehen muss.

Dabei untergraben hybride Angriffe beispielsweise auf Infrastruktur, Cyberraum und gesellschaftliche Stabilität klassische Verteidigungsstrategien. Die Grenzen zwischen innerer und äußerer Sicherheit verschwimmen, während globale Abhängigkeiten und technologische Entwicklungen die Bedrohungslage weiter verschärfen.

Deutschland kommt in diesem Kontext eine Schlüsselrolle zu. Durch die geografische Lage und die eigene wirtschaftliche Stärke spielt unser Land in den Verteidigungsplanungen der NATO eine zentrale Rolle als logistische „Drehscheibe“, Unterstützungszone für Verbündete und Bereitsteller von Streitkräften.

Gleichzeitig ist Deutschland ein bevorzugtes Ziel hybrider Angriffe durch Russland und andere systemische Rivalen. Diese Angriffe treffen Staat, Gesellschaft und Wirtschaft unterhalb der Schwelle militärischer Kampfhandlungen. Staatliche und nicht staatliche Akteur:innen nutzen systematisch bestehende Schwachstellen aus und bedienen sich dabei des gesamten Spektrums hybrider Angriffsmittel – etwa durch Desinformationskampagnen zur gesellschaftlichen Polarisierung oder durch gezielte Sabotageakte gegen kritische Infrastrukturen.

Rein militärische Verteidigung reicht somit als Ansatz nicht mehr aus. Um handlungsfähig zu bleiben, müssen alle Bereiche von Staat, Wirtschaft und Gesellschaft eingebunden werden. Sicherheit muss wieder als eine gesamtstaatliche und gesamtgesellschaftliche Aufgabe betrachtet werden, die eine umfassende und koordinierte Strategie erfordert – genau hier setzt das Analyseframework Comprehensive Defence an.

www.bwconsulting.de

7 Segmente Modell von Comprehensive Defence mit beispielhaften Handlungsfeldern:

Sieben eng miteinander verknüpfte und in Wechselwirkung stehende Segmente bilden den zentralen Ausgangspunkt des Frameworks Comprehensive Defence: Military, Social, Psychological, Digital, Civil, Economic und Ecological Defence.

Das Leitmotiv des Schirms verdeutlicht das für einen vollständigen Schutz notwendige Zusammenwirken aller Segmente. Halt bekommen sie durch funktionierende Verbindungen, die das Aufspannen des Schirms überhaupt erst ermöglichen. Die Mitte des Schirms steht für zentrale, übergeordnete Ansatzpunkte und Organisationen (wie die mögliche Koordinierungsstelle des Nationalen Sicherheitsrats), die den Segmenten eine gemeinsame Richtung geben, diese steuern und zusammenführen.

Das Framework richtet sich an alle handelnden Personen der Verteidigung sowohl in ihrer Gesamtheit als auch im Einzelnen – in Behörden und Organisationen aller Ressorts und Ebenen, in Unternehmen, in Nicht-Regierungsorganisationen (NGOs) und entsprechenden Verbänden sowie Initiativen.

Info: Total Defence beschreibt ein umfassendes Verteidigungskonzept, das während des Kalten Kriegs insbesondere von neutralen Staaten – beispielsweise in Skandinavien – entwickelt wurde. Es basiert auf der Einbindung der gesamten Gesellschaft in die nationale Sicherheit, wobei militärische Aspekte überwiegen. Bei Comprehensive Defence ist der militärische Aspekt einer von sieben gleichgewichteten Segmenten.

Denn wir sind überzeugt: Comprehensive Defence macht Deutschland widerstandsfähig und handlungsfähig – in stabilen Zeiten genauso wie in Krisen bis hin zum Krieg. Das Framework hilft Akteur:innen aus Staat, Wirtschaft und Gesellschaft, ihre Rollen und ihre Beiträge zur Gesamtverteidigung zu definieren und weiterzuentwickeln sowie Risiken und Lücken zu identifizieren und zu reduzieren.

Das Konzept setzt dabei auf ein fünfstufiges Vorgehen. Ausgehend von der Selbstverortung über Schnittstellenanalysen und strategische Zielbildung bis hin zur operativen Umsetzung und laufenden Anpassung ist es ein strategisches Instrument für eine nachhaltige Sicherheitsvorsorge. Es fördert ressortübergreifende Kooperation, klare Zuständigkeiten und eine koordinierte Sicherheitsstrategie.

Die Idee baut auf internationalen Modellen wie „Total Defence“ auf und ergänzt Planungsdokumente der NATO (auch hier findet sich der Begriff Comprehensive Defence), die Nationale Sicherheitsstrategie sowie die Verteidigungspolitischen Richtlinien durch eine gesamtstaatliche und gesamtgesellschaftliche Perspektive. Sie schafft die Grundlage für eine vernetzte, effektive Sicherheitsstruktur, in der alle Verantwortung übernehmen und einen Beitrag leisten.

Military Defence

Starke, gut ausgestattete und einsatzfähige Streitkräfte sowie gezielte militärische Strategien zur Abschreckung und zum Schutz des Landes.

Military Defence umfasst die Strategie, die Struktur und die Einsatzfähigkeit der Streitkräfte. Dazu gehören Ausrüstung, Ausbildung, Bündnisintegration und Mobilisierungsfähigkeit einschließlich Wehrpflicht und Reserve.
In Krisen und Krieg agieren sie nie isoliert, sondern ihre Erfolgsfähigkeit hängt von Verwaltung, Wirtschaft und Gesellschaft ab.

Internationale Partnerschaften sind essenziell für militärische Stärke, wobei strategische Koordinierung, Interoperabilität und gegenseitige Unterstützung die Verteidigungsfähigkeit sichern. Auch Rüstungspolitik, eine industrielle Basis und technologische Innovationskraft sind hierfür langfristig entscheidend. Anpassungsfähigkeit ist unerlässlich, ebenso wie das Überwinden bürokratischer Strukturen, die militärische Effizienz bremsen.

Aktuelle Lage und Herausforderungen

Nach Jahrzehnten der Fokussierung auf internationales Krisenmanagement steht seit dem russischen Angriffskrieg gegen die Ukraine die Landes- und Bündnisverteidigung wieder im Mittelpunkt. Um aktuelle Defizite der Einsatzbereitschaft aufzuholen, startete das Verteidigungsministerium auf Basis aktueller Szenarien verschiedene Initiativen, beispielsweise neue Gesetzgebungen für beschleunigte Beschaffungsverfahren.

Besonders die Fähigkeit, hoch intensive Kampfhandlungen durchzuhalten und hybride Kriegsführung zu bewältigen, ist auszubauen – Ausrüstung sowie Bestände an Material und Munition reichen dazu derzeit nicht aus.
Die deutsche Rüstungsindustrie wiederum ist technologisch leistungsfähig, benötigt aber klare Beschaffungsperspektiven.

Die gesellschaftliche Wahrnehmung der Bundeswehr verbessert sich, doch das Zusammenspiel von Militär und zivilen Strukturen bleibt herausfordernd. Personalmangel, fehlende Ausbildungskapazitäten und ungenutzte Potenziale für die Reserve erschweren die Mobilisierung. Gleichzeitig behindern langwierige Verwaltungsprozesse eine schnelle Anpassung an insbesondere hybride Bedrohungen.

Hybride Attacken nutzen gezielt diese Schwachstellen – militärische wie zivile – aus, während fehlende gemeinsame Informationsgrundlagen eine effektive Reaktion erschweren.

Erste Impulse für eine starke Military Defence

1. **Wehrpflicht denken & Reserve stärken:**
   Eine angemessene Truppenstärke wird durch neue Wehrpflichtformen sowie aktive und attraktive Reservistenarbeit inklusive regelmäßiger Übungen mit aktiven Streitkräften und zivilen Akteur:innen erreicht. Mobilisierungs- und Alarmpläne werden modernisiert, um im Krisen- oder Kriegsfall eine schnelle Rekonstitution zu gewährleisten.

2. **Verteidigungsindustrie fördern & Technologien weiterentwickeln:**
   Eine resiliente Verteidigungsindustrie mit innovativen Start-ups, mittelständischen Unternehmen und großen Konzernen, die über hohe und flexible Produktionskapazitäten sowie widerstandsfähige Prozesse verfügen, ist essenziell. Politik und Verwaltung stärken sie durch langfristige Beschaffungsverträge sowie eine proaktive Industriestrategie. Dies fördert nationale Beitragsmöglichkeiten innerhalb des Bündnisses, aber auch Autarkie. Rüstungsanforderungen werden flexibel gestaltet, Unternehmen können so ihre Rüstungsgüter während der Nutzung innerhalb weniger Wochen weiterentwickeln und anpassen.

Info: Der Krieg in der Ukraine hat gezeigt, dass die Innovationszyklen teilweise nur sechs Wochen betragen. Das bedeutet, dass Systeme oder ihre Software rasch überholt und weiterentwickelt werden müssen, da sie sonst einfacher aufgeklärt oder bekämpft werden können.

3. **Umfassende Abstimmung und strategische Kooperation ausbauen:**
   Verbündete und eigene Streitkräfte benötigen neben Ressourcen (z. B. Energie, Material) Wegefreiheit für Leistungen der Drehscheibe Deutschland und des Host Nation Support (HNS) – auch bei hohen Bedarfen in Krise und Krieg. Die Bundeswehr arbeitet hierfür eng mit anderen gesellschaftlichen und staatlichen Bereichen zusammen, um Operationsfreiheit zu sichern. Sie stärkt die Rolle der Verbindungskommandos.

4. **Nationale Sicherheitsstruktur effizient gestalten:**
   Der geplante Nationale Sicherheitsrat sowie der koordinierende Krisenstab zeichnen sich durch klare Zuständigkeiten, schnelle Entscheidungsprozesse und ausreichende personelle Ressourcen aus. Ein übergreifendes Schnittstellenmanagement mit transparenter Kommunikation und klaren Verantwortlichkeiten verbessert die Zusammenarbeit zwischen militärischen, zivilen und wirtschaftlichen Akteuren.

5. **Digitalisierung forcieren:**
   Ein umfassendes, digital vernetztes Lagebild, das alle sicherheitsrelevanten Daten aus Behörden, Militär, Geheimdiensten und Wirtschaft zusammenführt, bildet die Grundlage für schnelle, abgestimmte Entscheidungen.

„Military Defence gelingt im Verbund – im Bündnis und mit Partnernationen, ressortübergreifend sowie in enger Kooperation mit Wirtschaft und Wissenschaft. Die Bundeswehr muss dafür die Möglichkeiten technologischer Entwicklung für Innovationen nutzen und Hürden der Bürokratie überwinden.“

Wolfgang Gäbelein
Generalmajor a. D.
Senior Expert bei der BwConsulting

Social Defence

Starker gesellschaftlicher Zusammenhalt und ein kollektives Gemeinschaftsgefühl schaffen Engagement und Resilienz.

Social Defence stärkt die kollektive Widerstandsfähigkeit der Gesellschaft gegenüber modernen Bedrohungen, Krisen und Kriegen. Im Fokus stehen der soziale Zusammenhalt aller Menschen in Deutschland, der Umgang mit unterschiedlichen Informationsräumen und die Überwindung gesellschaftlicher Spaltungen.

Denn eine vielfältige, aber geeinte Gesellschaft kann Krisen und hybriden Angriffen resilient begegnen, sich an neue Herausforderungen anpassen und gezielte Destabilisierungsversuche entschlossen abwenden.

Aktuelle Lage und Herausforderungen

Deutschland zeichnet sich durch eine hohe gesellschaftliche Vielfalt aus, die eine demokratische Stärke darstellt. Das gesamtgesellschaftliche Zusammengehörigkeitsgefühl ist jedoch leicht angreifbar und somit eine potenzielle Angriffsfläche für hybride Bedrohungen wie gezielte Desinformationskampagnen.

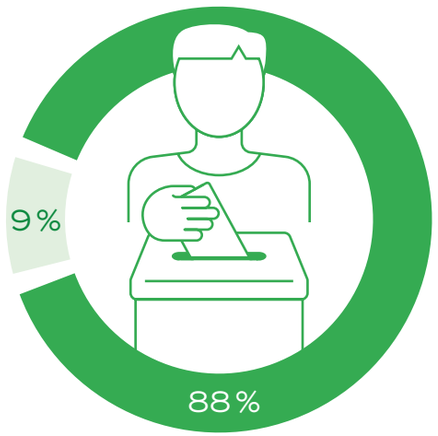
Obwohl die Demokratie individuelle Freiheit zur politischen und gesellschaftlichen Beteiligung bietet, ist das Engagement in Ehrenamt und Vereinen rückläufig. Gleichzeitig führt die zunehmende digitale Vernetzung zu Anonymität und Fragmentierung in Informationsblasen, wodurch der direkte soziale Austausch abnimmt.

Wirtschaftliche Unsicherheiten, geopolitische Spannungen und steigende Lebenshaltungskosten verstärken gemeinsam mit der polarisierenden Wirkung von Social-Media-Algorithmen die gesellschaftliche Entzweiung, schaffen gesellschaftliche Polarisierung und sorgen für Misstrauen gegenüber staatlichen Institutionen und Mechanismen. Auch die Spaltung zwischen verschiedenen sozioökonomischen Gruppen nimmt zu und stellt eine wachsende Herausforderung für die gesellschaftliche Stabilität dar.

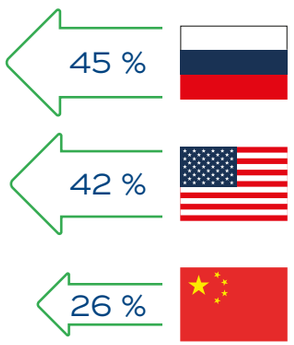
Furcht vor Desinformationskampagnen bei Bundestagswahlen

9 %
der Stimmberechtigten glauben nicht an eine Einflussnahme von außen über Social Media.

88 %
der Stimmberechtigten befürchten Einflussnahme von außen über Social Media.



Verdachte der Stimmberechtigten:



Quelle: https://www.bitkom.org/Presse/Presseinformation/Bundestagswahl-Grosse-Mehrheit-fuerchtet-Einflussnahme-Ausland

Erste Impulse für eine starke Social Defence

1. **Gesellschaftliche Verankerung fördern:**
   Die Förderung von Ehrenamt, sozialen und militärischen Diensten sowie Vereinsmitgliedschaften führt weg von individuellem Egoismus und digitaler Anonymität hin zu greifbaren Gemeinschaften. Wenig bürokratische Prozesse für die Anerkennung von Ehrenämtern durch Arbeitgebende sowie steuerliche Anreize unterstützen die Attraktivität gesellschaftlichen Engagements.

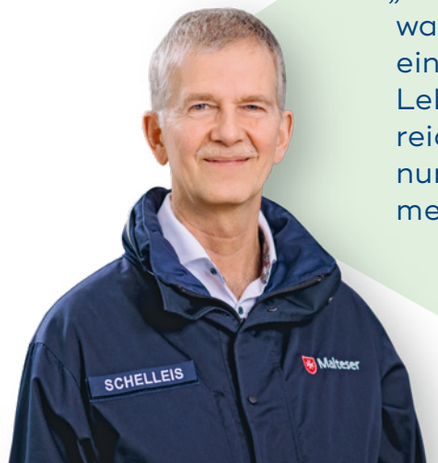
2. **Demokratische Teilhabe ausbauen:**
   Instrumente wie beschleunigte Verwaltungsakte, die Weiterentwicklung von Bürgerräten, eine temporär zugeloste Parlamentskammer oder ein Ausschuss für Demokratiepolitik sowohl in Deutschland als auch auf EU-Ebene stärken politische Beteiligung.

3. **Soziale Gerechtigkeit sicherstellen:**
   Das Prinzip des sozialen Bundesstaats gemäß Artikel 20 des Grundgesetzes wird unter Berücksichtigung eventueller Krisen- und Kriegsszenarien weitergedacht. Politik und Arbeitgebende verfolgen vor diesem Hintergrund strukturell die Abfederung von wirtschaftlichen und sozialen Ungleichheiten. Die Versorgung von hilfebedürftigen Menschen und Geflüchteten wird vorbereitet, wobei Transparenz das Vertrauen in staatliche Verteilungsmechanismen stärkt, die auch in Krise und Krieg funktionieren müssen.

4. **Gemeinschaftsgefühl stärken:**
   Gezielte Bildungsprogramme, symbolische Rituale und interkulturelle Begegnungen fördern das Miteinander und überwinden Unterschiede, ohne die Vielfalt einzuschränken. Nachbarschaftsinitiativen, NGOs und lokale Netzwerke sind dabei essenziell für gesellschaftlichen Zusammenhalt.

   Info: Ein Beispiel für die Stärkung des Gemeinschaftsgefühls ist das Projekt „S17 Community Kitchen“ in Singapur, das lokal günstige Mahlzeiten anbietet und gleichzeitig eine Plattform für soziale Interaktion und Unterstützung innerhalb der Nachbarschaft bildet.

5. **Resilienz durch gezielte Investitionen erhöhen:**
   Programme zum Aufbau der kollektiven Widerstandsfähigkeit, zur Stärkung des Gemeinschaftssinns und zum aktiven Diskurs über Sicherheitspolitik werden aufgebaut, um das gemeinsame Bewusstsein für Verantwortung und Bedrohungslage nachhaltig zu erzeugen.



„Wir müssen uns als Gesellschaft klarmachen, was wir verteidigen wollen. Ein bloßes Nebeneinanderher von politischen Ansichten, Lebensentwürfen und Partikularinteressen reicht dazu nicht hin. Es braucht mehr als nur den kleinsten gemeinsamen Nenner – mehr Gemeinsinn!“

Martin Schelleis
Malteser Bundesbeauftragter für Krisenresilienz

Psychological Defence

Resiliente Individuen sind Grundlage einer verteidigungsfähigen Gemeinschaft.

Psychological Defence stärkt gezielt die Widerstandsfähigkeit des einzelnen Individuums gegenüber hybriden Angriffen, Krisen und Kriegen. Sie setzt auf individuelle Resilienz und Selbstschutzfähigkeit, um Manipulation und Destabilisierung vorzubeugen. Dafür muss auch das persönliche Vertrauen der Menschen in Staat und Institutionen – trotz hybrider Bedrohungen und Desinformation – gestärkt werden.

Psychological Defence spielt insbesondere in hybriden Szenarien eine zentrale Rolle – ihre Wirksamkeit hängt jedoch maßgeblich davon ab, dass sie bereits in Friedenszeiten strategisch aufgebaut und verankert wird. Eine nachträgliche Implementierung in Krise oder Krieg ist nur bedingt möglich und deutlich weniger wirkungsvoll. Transparente Kommunikation, nachvollziehbare Narrative und hohe Glaubwürdigkeit von öffentlichen Medien sind essenziell, um Demokratie und gesellschaftliche Stabilität zu sichern.

Psychological Defence fördert eine informierte, widerstandsfähige Bevölkerung, die Bedrohungen und Desinformation erkennt, ihnen aktiv begegnet und ihre demokratischen Werte entschlossen verteidigt.

Aktuelle Lage und Herausforderungen

Deutschland ist vom Individualismus geprägt, oft erklärt mit dem wirtschaftlichen Wandel und neoliberalen Prinzipien. Wichtige Errungenschaften für die persönlichen Freiheiten werden gesehen, jedoch oft nicht die Pflichten, die damit einhergehen. Damit verbunden ist zudem ein wachsendes Misstrauen in staatliche Institutionen. Ein sicherheitspolitisches Bewusstsein ist in der deutschen Bevölkerung eher gering ausgeprägt.

Staatliche Vorgaben werden häufig als Einschränkung empfunden, während Eigennutz und undemokratische Tendenzen zunehmen. Gleichzeitig prägt ein hohes Sicherheitsbedürfnis die Menschen in Deutschland, beschrieben als „German Angst“. Die Überwindung dieses Zwiespalts stellt eine Herausforderung für individuelle und gesellschaftliche Resilienz dar.

Erste Impulse für eine starke Psychological Defence

1. **Vertrauen in Staat und Institutionen festigen:**
   Handelnde auf allen föderalen Ebenen kommunizieren bewusst verständlich und zielgruppenorientiert. Vor-Ort-Angebote zur politischen Bildung an alle Gesellschaftsschichten stärken das Vertrauen in demokratische Strukturen und verbessern die individuelle Resilienz gegenüber Manipulation.

2. **Desinformation aktiv bekämpfen:**
   Effektive und wahrnehmbare rechtliche Maßnahmen gegen Falschmeldungen, schnelle Faktenchecks durch öffentliche Medien und Behörden sowie (Desinformations-)Frühwarnsysteme helfen, gezielte Manipulation frühzeitig zu erkennen und effektiv abzuwehren.

3. **Kritisches Denken fördern:**
   Gezielte Aufklärung auf allen Bildungswegen, an Arbeitsplätzen und in der Ehrenamtsfortbildung sensibilisieren Bürger:innen dafür, Informationen sowie Narrative kritisch zu hinterfragen und Desinformationskampagnen zu entschärfen.

4. **Resilienz durch Krisenvorbereitung steigern:**
   Regelmäßige Sicherheitsübungen in Schulen und Betrieben, öffentlichkeitswirksame Tests und die Weiterentwicklung von Warnsystemen sowie leicht verständliche Kriseninformationen stärken die Handlungsfähigkeit der Bevölkerung im Ernstfall.

Info: Schweden hat eine Broschüre „In case of crisis and war“ an alle Einwohner:innen verteilt, die nicht nur den Katastrophenschutz, sondern explizit auch das Verhalten bei hybriden und militärischen Angriffen thematisiert. Ausdrücklich sind alle Menschen in Schweden unabhängig von der Staatsbürgerschaft zwischen 16 und 70 Jahren in das Verteidigungskonzept eingebunden.

5. **Psychische Widerstandsfähigkeit ausbauen:**
   Inhalte in Schul- und Berufsbildung, Gesundheitsvorsorge und psychologische Notfallversorgung werden gezielt weiterentwickelt, um Menschen zu befähigen, mit Angst, Stress und Trauma vor und in Krisensituationen umzugehen.

„Die Verbesserung der Psychological Defence ist von allen Verteidigungsarten wohl das dickste Brett. Politik muss beweisen, dass sie handlungswillig ist, groß denkt und den Staat reformieren kann.“

Prof. Dr. Sönke Neitzel
Professor für Militärgeschichte/Kulturgeschichte der Gewalt an der Universität Potsdam

Digital Defence

Cybersicherheit schützt den digitalen Raum und eine digitalisierte, vernetzte Gesellschaft.

Digital Defence schützt den gesamten digitalen Raum in Wirtschaft, Staat und Gesellschaft vor IT-spezifischen Bedrohungen sowie deren Auswirkungen. Denn kein Bereich ist stärker international vernetzt und zugleich abhängiger von globalen Entwicklungen. Voraussetzung für digitale Souveränität ist eine robuste, diversifizierte und unabhängige Infrastruktur mit eigenen Fähigkeiten, die trotz geopolitischer Verschiebungen stabil bleibt.

Gleichzeitig sind Desinformation und Destabilisierung digitale Wege, um kinetische Angriffe vorzubereiten – deshalb ist der Aufbau eines resilienten Cyberraums entscheidend. Er benötigt technisch wie regulatorisch stabile, funktionierende Rahmenbedingungen.

Aktuelle Lage und Herausforderungen

Die zunehmende Digitalisierung bringt eine komplexe Bedrohungslage mit sich. Cyberangriffe nehmen zu, werden technisch ausgefeilter und oft von staatlichen Einrichtungen oder organisierten kriminellen Gruppen gesteuert. Die Anonymität des Internets erschwert eine eindeutige Zuordnung cyberbasierter Angriffe erheblich, da Angreifende ihre Spuren gezielt verschleiern können. Obwohl sich solche Angriffe in der Regel unterhalb der Schwelle eines bewaffneten Konflikts bewegen, können sie dennoch erhebliche sicherheitspolitische, wirtschaftliche und gesellschaftliche Wirkungen entfalten.

Fragmentierte Zuständigkeiten, Fachkräftemangel und ein geringes Bewusstsein für Risiken in Bevölkerung und Wirtschaft – bisweilen auch konträre wirtschaftliche Anreize – erschweren die Cyberabwehr. Internationale Zusammenarbeit ist herausfordernd, da Angreifende Unterschiede und mangelnde Kommunikation zwischen Strafverfolgungsbehörden gezielt ausnutzen.

Zudem ist Europa stark von außereuropäischen Technologien abhängig – insbesondere von US-amerikanischen Dienstleistern und deren digitaler Infrastruktur. Diese Abhängigkeit gefährdet die Informationssouveränität und macht Europa verwundbar gegenüber externen Einschränkungen.

Die Verarbeitung vertraulicher und sensible Daten sowie geistigen Eigentums ist zwar essenziell zur Aufrechterhaltung von vielen Dienstleistungen, diese Prozesse sind aber auch vielfach bedroht, etwa durch Datenabfluss bei der Nutzung von Cloud-Diensten. Zudem erschwert die Dominanz nicht europäischer Plattformen die medienrechtliche Kontrolle, fördert Desinformation und ermöglicht autoritären Gruppen, gesellschaftliche Diskurse zu manipulieren.

Neue Technologien wie künstliche Intelligenz und Quanten-Computing verschärfen die Problematik weiter, da deren Entwicklung und Nutzung aktuell ebenfalls meist von US-amerikanischen oder chinesischen Unternehmen abhängt. Der Aufbau unabhängiger europäischer Kompetenzen wird dadurch zunehmend schwieriger.

Erste Impulse für eine starke Digital Defence

1. **Digitale Resilienz durch Bildung und Einbindung fördern:**
   Deutschland orientiert sich an internationalen Best Practices und einem „Whole-of-Society"-Ansatz, der die gesamte Gesellschaft (Individuen, Unternehmen, staatliche Institutionen, Medien etc.) in die Cyberabwehr einbezieht und hierfür Schulungsprogramme und Anreize für die Bevölkerung sowie Behörden und Unternehmen etabliert. IT-Sicherheitskompetenzen werden frühzeitig, beispielsweise im Schulunterricht, vermittelt, jedoch auch in späteren Phasen des Lebens konstant weiterentwickelt.

2. **Digitale Souveränität stärken & Abhängigkeiten reduzieren:**
   Europa fördert eigene Technologien und bietet politische Unterstützung für europäische Softwareinitiativen. Entscheidend sind die praktische Anwendung und die Skalierbarkeit als konkretes Ergebnis der theoretischen Forschung. Sicherheitsstandards wie „Security by Design" und regelmäßige Code-Audits werden verpflichtend.

3. **IT-Infrastruktur absichern & Angriffsflächen minimieren:**
   Eine dezentrale Infrastruktur sowie sicherheitsfördernde Architekturen (Zero Trust, Netzsegmentierung, quantensichere Verschlüsselung) werden priorisiert gefördert. Hochwertige Softwarequalitätssicherung und regelmäßige Sicherheitsüberprüfungen werden für öffentliche IT-Systeme obligatorisch.

4. **Koordination und Reaktionsfähigkeit verbessern:**
   Die Rolle des Bundesamts für Sicherheit in der Informationstechnik (BSI) als zentraler Akteur in der deutschen Cybersicherheitsarchitektur wird gestärkt. Integrierte Cyber Emergency Response Teams (CERTs) aus BSI und anderen staatlichen wie privaten Einrichtungen werden besser koordiniert und tragen entscheidend zur Krisenbewältigung bei. Darüber hinaus dämmt eine zielgerichtete öffentliche Krisenkommunikation bei breit wirkenden Cybervorfällen über reichweitenstarke Medien den Schaden ein.

Info: Cyber Emergency Response Team (CERT) oder Computer Security Incident Response Team (CSIRT) bezeichnet eine Gruppe von IT-Sicherheitsfachleuten, die auf die Bewältigung von Cybersicherheitsvorfällen spezialisiert ist.
Aktuell existiert beispielsweise beim BSI das BürgerCERT, das sich an die Bevölkerung sowie kleinere Unternehmen richtet. Es informiert kostenlos und neutral über aktuelle Gefahren wie Schadsoftware und Sicherheitslücken in Computersystemen. Daneben gibt es das CERT-Bund mit einem besonderen Fokus auf die bundesbehördliche Cybersicherheit.

5. **Angreifende konsequent aufklären und attribuieren:**
   Die Fähigkeiten zur koordinierten Aufklärung von Angriffen im Cyberraum werden (analog zu anderen staatlichen Schutzbereichen) auf- und ausgebaut. Ein Sanktionsregime für die Einschränkung von Wirtschaftsbeziehungen bei staatlich gesteuerten Angriffsszenarien wird eingerichtet.

„Cybersecurity ist Teamsport. Jedes Glied in der Kette zählt – von Oma mit ihrem Smartphone bis zum Konzern-CEO. Wir brauchen eine digitale Alphabetisierung und Verantwortungsübernahme für alle, nicht nur für IT-Profis."

Manuel ‚HonkHase' Atug
IT-Sicherheitsexperte

Civil Defence

Ein starker Zivil- und Katastrophenschutz ist essenziell für den Schutz und die Grundversorgung der Zivilbevölkerung.

Civil Defence bereitet die Bevölkerung und die Infrastruktur eines Landes auf Katastrophen, Krisen und Krieg vor. Ziel ist es, deren Auswirkungen zu minimieren und die Funktionsfähigkeit des gesellschaftlichen Alltags zu sichern. Dafür benötigt es einen hocheffektiven Katastrophen- und Zivilschutz sowie die polizeiliche Gefahrenabwehr. Hinzu kommt ein breites Bewusstsein für individuelle sowie kollektive Vorsorgemaßnahmen. Eine funktionierende Notfallkommunikation sowie die Aufrechterhaltung demokratischer Strukturen in Krisenfällen sind dabei für Civil Defence essenziell.

Entscheidend ist die enge Zusammenarbeit zwischen Staat, privaten Organisationen und Freiwilligen, um Ressourcen effizient zu bündeln und im Ernstfall schnell, koordiniert und entschlossen handeln zu können sowie gleichzeitig die öffentliche Ordnung bestmöglich aufrechterhalten zu können.

Aktuelle Lage und Herausforderungen

Der Zivilschutz in Deutschland wurde nach dem Kalten Krieg stark reduziert, Schutzkapazitäten wie Bunkeranlagen wurden abgebaut, und das Bundesamt für Zivilschutz wurde 1999 aufgelöst. Trotz wachsender Bedrohungen bleiben die Mittel für Bevölkerungsschutz gering, wodurch die aktuelle Sicherheitslage unzureichend adressiert wird.

Während der Zivilschutz dem Bund unterliegt, verantworten Länder und Kommunen den Katastrophenschutz – eine komplexe Struktur, die in Krisen zu Koordinationsproblemen führt. Feuerwehr, Polizei und freiwillige Rettungsdienste arbeiten zwar eng zusammen, jedoch erschweren begrenzte Haushaltsmittel, Personalmangel, technische Kompatibilitätsprobleme, unzureichender Informationsaustausch und die Belastung im Ehrenamt die Einsatzfähigkeit.

Die zunehmenden Herausforderungen, darunter klimabedingte Krisen und hybride Bedrohungen, erfordern eine verbesserte Finanzierung, klare Zuständigkeiten und gestärkte Notfallstrukturen.

Bevölkerungsschutz als Oberbegriff für Zivil- und Katastrophenschutz

Bevölkerungsschutz

Oberbegriff für Maßnahmen, die den Schutz der Bevölkerung vor Gefahren im Spannungs- oder Verteidigungsfall oder im Katastrophenfall zum Ziel haben.

Zivilschutz

Schutz von Bevölkerung, Betrieben und öffentlichen Einrichtungen im Spannungs- oder Verteidigungsfall durch nicht militärische Maßnahmen. Die Zuständigkeit für den Zivilschutz liegt beim Bund.

Katastrophenschutz

Schutz von Menschen, Sachgütern und Umwelt vor dem Eintritt und den Folgen einer Katastrophe. Sie liegt vor, wenn ein Schadensfall nicht im Rahmen der Alltagsorganisation bewältigt werden kann und eine zentrale Steuerung der Maßnahmen erforderlich ist. Die Zuständigkeit liegt bei Ländern und Kommunen.

Quelle: www.bbk.bund.de

Erste Impulse für eine starke Civil Defence

1. **Paradigmenwechsel einleiten – „Just in Case“ statt „Just in Time“:**
   Die Bevölkerung und kritische Infrastrukturen werden als aktive, sich selbst schützende Akteurinnen verstanden, nicht als schutzbedürftige Objekte. Regelmäßige Informationskampagnen zu den Themen Notfallvorsorge, Versorgungssicherheit und Schutzmaßnahmen sowie Zivilschutzübungen mit staatlichen Stellen stärken das Know-how zur Selbstversorgung über einen bestimmten Zeitraum.

2. **Moderne Schutzrauminfrastruktur aufbauen:**
   Deutschland investiert wieder in den Ausbau von Schutzräumen. „Dual-Use“-Ansätze für diese Schutzanlagen werden dabei mitgedacht, denn sie stärken auch die Wirtschaftlichkeit in Friedenszeiten (beispielsweise Sportstätten, Tiefgaragen, U-Bahn-Stationen).

3. **Ehrenamt und gerechte Helfergleichstellung stärken:**
   Eine bundeseinheitliche Helfergleichstellung für Ehrenamtliche im Bevölkerungsschutz (Feuerwehr, Technisches Hilfswerk, Deutsches Rotes Kreuz etc.) sowie attraktive Anreize zum Eintritt und zur langfristigen Bindung von Freiwilligen werden aufgesetzt. Neben gesetzlichen Regelungen zur Freistellung im Übungs- und Einsatzfall, analog zu Reservist:innen der Bundeswehr, sind zusätzliche Urlaubstage, kostenlose Qualifikationen oder Vorteile bei öffentlichen Dienstleistungen weitere Anreize zur langfristigen Bindung von Freiwilligen.

Info: Mit knapp 370.000 privaten und öffentlichen Schutzräumen stellt die Schweiz einen umfänglichen Schutz von über 100 % ihrer eigenen Bevölkerung sicher, und in Finnland werden große Bunkeranlagen in Friedenszeiten als Tiefgaragen oder Sportplätze genutzt.

4. **Effiziente Einsatzkoordinierung und Frühwarnsysteme etablieren:**
   Frühwarnsysteme mit automatisierter Sammlung und Auswertung werden etabliert, um notwendige Informationen an beteiligte Organisationen sowie die betroffene Bevölkerung zu verteilen. Ad-hoc-Einsatzstäbe mit definierten Mitgliedern bzw. feste Krisenorganisationen werden daneben mit klaren Zuständigkeiten und Entscheidungsbefugnissen ausgestattet, um eine effektive Einsatzkoordination zwischen den diversen Organisationen und Ebenen sicherzustellen unter bestmöglicher Aufrechthaltung der öffentlichen Ordnung. Aus Daten vergangener Katastrophenlagen in In- und Ausland werden Best Practices identifiziert und in bestehende Bevölkerungsschutzstrategien implementiert.

5. **Öffentliche Sicherheit trainieren:**
   Zum Schutz der Zivilbevölkerung in Friedens-, hybriden Bedrohungs- und Krisenszenarien koordinieren und üben die Sicherheitsbehörden ihre Arbeit eng – auch über föderale Grenzen hinweg. Gerade bei hybriden Attacken kann es zu unübersichtlichen Lagen kommen, die Polizeibehörden bereiten sich hierauf vor – ebenso die Einsatzkräfte von weiteren Blaulichtorganisationen wie Feuerwehr, THW und Rettungssanitätsdiensten. Für alle diese Kräfte besteht das Risiko, wie Beispiele aus der Ukraine zeigen, im Kriegsfall selbst zum Angriffsziel zu werden, daher werden für sie bestmögliche Schutzmaßnahmen geplant und trainiert.

„Das Framework macht sichtbar: Verteidigung funktioniert nur gemeinsam. Es hilft uns zu verstehen, welche Partner wir zur Civil Defence brauchen und wie wir gemeinsam resiliente Strukturen aufbauen können – von den Kommunen über die Länder bis hin zum Bund.“

Prof. Dr. Christian Dusch
Landrat des Landkreises Rastatt

Economic Defence

Wirtschaftliche Leistungsfähigkeit und Widerstands-kraft ermöglichen Wachstum und Stabilität bei Disruption und Bedrohungen.

Economic Defence sichert die wirtschaftliche Widerstandsfähigkeit eines Landes gegen geopolitische Spannungen, Krisen und Kriege. Sichere Lieferketten, wirtschaftliche Diversifizierung, die Verfügbarkeit von Rüstungsgütern, Cyberresilienz und die Unabhängigkeit von feindlich gesinnten Akteur:innen spielen hier eine zentrale Rolle, um Stabilität zu gewährleisten.

Denn eine starke Wirtschaft bildet das Fundament für sozialen Wohlstand und nationale Sicherheit. Sie muss auch im Ernstfall die allgemeine Versorgung der Bevölkerung aufrechterhalten und gleichzeitig die Produktion verteidigungsrelevanter Güter im erhöhten Umfang sicherstellen können.

Nur ein widerstandsfähiges, flexibles Zusammenspiel zwischen Staat, Wirtschaft und Gesellschaft kann auf unvorhersehbare Bedrohungen reagieren und langfristig Sicherheit gewährleisten.

Aktuelle Lage und Herausforderungen

Die globale Wirtschaft steht unter Druck: Handelskonflikte, geopolitische Spannungen und volatile Märkte gefährden Lieferketten und Rohstoffversorgung. Besonders kritische Infrastrukturen und Industrien wie der Energie- und Gesundheitssektor sind anfällig für externe Störungen. Deutschland ist zudem als Exportnation stark von internationalen Lieferketten, Währungsschwankungen und Energieimporten abhängig.

Dabei ist die Krisenvorsorge unzureichend – strategische Notfallreserven für Lebensmittel, Medizin, Schutzausrüstung, kritische Ressourcen und Bauteile sowie Energie sind kaum vorhanden. Zudem kämpfen kleine und mittlere Unternehmen mit begrenzten Ressourcen für Cyberabwehr und IT-Sicherheit, was ihre Widerstandsfähigkeit zusätzlich schwächt.

„Störungen in Lieferketten oder Cyberangriffe sind für uns alltägliche Risiken, keine Theorie. Dafür benötigt man eine vorausschauende Planung sowie Kooperationen, um resiliente Lieferketten schon heute und nicht erst im Ernstfall sicherzustellen."

Stefan Weiser
Senior Principal Defense,
Aerospace & Industry – SCHOTT AG

Erste Impulse für eine starke Economic Defence

1. **Strategische Notfallreserven und Notfallfonds ausbauen:**
   Unternehmen (insbesondere der Lebensmittelhandel) und der Staat schaffen koordiniert größere und rollierende Lager mit strategischen Notfallreserven für kritische Güter, um Engpässen vorzubeugen. Ein Notfallfonds, analog zu skandinavischen Modellen, wird aufgesetzt, um insbesondere kleinen und mittleren Unternehmen gezielte Unterstützung in Krisenzeiten zu bieten.

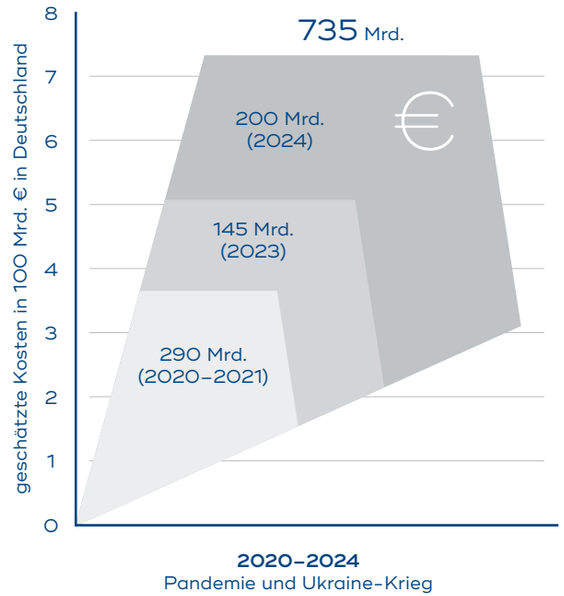
Info: Die Schweiz verpflichtet Unternehmen zur Lagerung lebenswichtiger Güter, etwa Lebensmittel, Medikamente, Treibstoffe, Düngemittel und Saatgut. In Finnland gibt es ebenfalls gesetzlich vorgeschriebene Vorräte für Unternehmen. Dort werden die Verteilungssysteme der strategischen Notfallreserven sogar regelmäßig beübt.

2. **Wirtschaft diversifizieren & Lieferketten resilient gestalten:**
   Stärkere wirtschaftliche Unabhängigkeit insbesondere in der IT- und Digitalwirtschaft, aber auch in der Rüstungsindustrie, federt externe Erschütterungen beispielsweise von vulnerablen Lieferketten besser ab. Daneben fördert eine wesentliche Entbürokratisierung Innovation und treibt die Diversifizierung von Märkten an.

3. **Unternehmenssicherheit stärken:**
   Unternehmen werden intensiver in staatliche Krisenübungen integriert. Neu aufgesetzte Schulungs- und Beratungsprogramme helfen insbesondere kleinen und mittleren Unternehmen, ihre Widerstandskraft gegenüber Cyberangriffen und wirtschaftlichen Krisen zu erhöhen. Eine umfassende systematische Analyse der Schwachstellen im deutschen Wirtschafts- und Finanzsystem identifiziert und reduziert darüber hinaus konstant bestehende Angriffsflächen.

4. **Kritische Infrastruktur gezielt schützen:**
   Konzepte und Regulierungen zum Schutz kritischer Infrastrukturen werden weiter operationalisiert, um eine zuverlässige Versorgung mit Energie, Lebensmitteln, Arzneimitteln und auch Rüstungsgütern sicherzustellen.

Krisenbedingte ökonomische Verluste



Quelle zur Grafik:
IW Köln: https://www.iwkoeln.de/en/studies/michael-groemling-the-economic-losses-in-germany-due-to-the-pandemic-and-the-war-in-ukraine.html

Ecological Defence

Durch nachhaltigen Schutz und Anpassungsfähigkeit Lebensgrundlagen schützen.

Ecological Defence sichert die natürlichen Lebensgrundlagen der Bevölkerung und stärkt die Resilienz gegenüber Umweltveränderungen. Ziel ist der Schutz von Klima, Natur und Ressourcen – auch im Hinblick auf ihre strategische Bedeutung für die Krisenvorsorge und die Verteidigungsfähigkeit. Nachhaltigkeit und Umweltschutz werden damit zu sicherheitspolitischen Faktoren.

So soll Ecological Defence umweltbedingte Risiken abschwächen und nachhaltige Strukturen sowohl für die Krisenfestigkeit als auch für die Verteidigungsfähigkeit schaffen sowie die strategische Abhängigkeit von umweltschädlichen bzw. knappen Ressourcen verringern. Erneuerbare Energien, Ressourceneffizienz und ein vorausschauender Umgang mit Natur und Infrastruktur sind zentrale Elemente.

Aktuelle Lage und Herausforderungen

Der Klimawandel verstärkt Risiken wie Extremwetter, Naturkatastrophen, Wassermangel oder den Verlust fruchtbarer Böden. Diese Ereignisse gefährden kritische Infrastrukturen, verursachen Versorgungsengpässe und verschärfen bestehende Krisen.

Indirekte Folgen wie Fluchtbewegungen aufgrund von lokalen Krisen sowie Konflikte um Ressourcen erhöhen geopolitische Spannungen. Auch Kriege selbst, wie aktuell in der Ukraine, führen zu großflächigen Umweltschäden mit langfristigen Auswirkungen auf Gesundheit, Landwirtschaft und Versorgung.

Deutschland erkennt den Schutz der Lebensgrundlagen in der Nationalen Sicherheitsstrategie als sicherheitsrelevant an. Dennoch fehlt es an konkreten Umsetzungsstrategien. Gleichzeitig steigen die Anforderungen an den Umwelt- und Klimaschutz – auch im Verteidigungssektor. Naturkatastrophen wie das Ahrtal-Hochwasser zeigen Schwächen in Prävention, Reaktion und Wiederaufbau. Zudem konkurrieren ökologische Maßnahmen teils untereinander, teils mit sicherheitspolitischen Prioritäten wie der kurzfristigen Erhöhung der Einsatzbereitschaft oder Erlösmaximierung in der Wirtschaft.

Die Bundeswehr hat 2023 und 2024 erste Strategien zu Nachhaltigkeit und Klimaschutz sowie zum Umgang mit dem Klimawandel veröffentlicht. Eine systematische Integration in Planung, Beschaffung und Übungspraxis steht aber noch am Anfang. Dabei könnte Deutschland – auch im internationalen Vergleich – eine Vorreiterrolle einnehmen.

Erste Impulse für eine starke Economic Defence

1. **Erneuerbare Energien und energetische Souveränität stärken:**
   Der kontinuierliche Ausbau erneuerbarer Energien erhöht die kontinuierliche Resilienz kritischer Infrastrukturen, reduziert Abhängigkeiten von fossilen Energieträgern und verringert zudem Treibhausgasemissionen. Bestehende Infrastrukturen – etwa Liegenschaften von Bund, Ländern und Gemeinden – bieten Potenziale für Photovoltaik, Geothermie oder Begrünung.

2. **Lebensgrundlagen sichern & Frühwarnsysteme ausbauen:**
   Kritische Naturressourcen wie Gewässer, Wälder oder landwirtschaftliche Flächen sowie (kritische) Infrastrukturen werden besser geschützt. Multisensorale Überwachung, Deichschutz, dezentrale Strukturen und Frühwarnsysteme erhöhen die Reaktionsfähigkeit bei Gefahren für Natur und Mensch.

3. **Nachhaltige Beschaffung und grüne Leitmärkte fördern:**
   Die Bundeswehr integriert Umweltkriterien in ihre Beschaffungsprozesse und unterstützt gezielt umweltfreundliche Technologien. So entwickelt und stärkt sie nachhaltige Leitmärkte auch in der Sicherheits- und Rüstungsindustrie.

4. **Innovation und Biodiversität nutzen:**
   Der Einsatz moderner Technologien wie „Internet of Things“ (IoT), Satellitenaufklärung oder KI verbessert Risikoerkennung und Krisenreaktion. Gleichzeitig sind Biodiversität und ökologische Vielfalt essenziell für Ernährung, Medizin und Resilienz – auch im Verteidigungsfall.

Info: Der Krieg in der Ukraine verdeutlicht dramatisch die unmittelbaren Effekte auf Natur und Lebensgrundlagen: Zahlreiche Waldbrände, Verminung und Verseuchung von Gebieten und Gewässern (unter anderem durch Schwermetalle, Sprengstoffe und zerstörtes Material), der Einsatz chemischer Waffen oder die durch eine Dammsprengung ausgelöste Überflutung sind eine Belastung für die Umwelt und bedrohen überlebenswichtige natürliche Lebensgrundlagen.

„Dauerhafte Verteidigung bedingt den Zugriff auf alle Arten von Ressourcen. Neben Personal und Gerät zählen dazu auch Energie und weitere Rohstoffe. Energieautonome und -souveräne Streitkräfte sind deshalb nachhaltig und operativ einsatzfähiger.“

Prof. Dr. Stefan Bayer
Leiter Forschung
German Institute for Defence and Strategic Studies

Was kann getan werden?

Vorgehen in fünf Schritten zur Anwendung von Comprehensive Defence in der eigenen Organisation.

Comprehensive Defence erfordert eine gesamtstaatliche und gesamtgesellschaftliche Herangehensweise, bei der alle Beteiligten zusammenwirken, um Sicherheit und Widerstandsfähigkeit nachhaltig zu gewährleisten.

Uns ist bewusst: Die Implementierung dieses Ansatzes ist komplex. Aber notwendig, um sich auf zukünftige Krisen, hybride Bedrohungen und geopolitische Spannungen vorzubereiten.

Verantwortliche können anhand einer klaren Struktur in fünf Schritten vorgehen, um Comprehensive Defence systematisch in der eigenen Organisation umzusetzen:

1. **Die eigene Organisation im Rahmen der Gesamtverteidigung analysieren**
   Leitfrage: Was trägt die eigene Organisation bzw. das eigene Unternehmen in den Segmenten bei, und was könnte zukünftig jeweils beigetragen werden?

   Alle handelnden Personen sollten die eigene Bedeutung für die Gesamtverteidigung analysieren und ihre Schwerpunkte in den Segmenten der Comprehensive Defence identifizieren. Auch in scheinbar nicht sicherheitsrelevanten Bereichen können essenzielle Beiträge geleistet werden – sei es durch Infrastruktur, Kommunikation, Logistik oder wirtschaftliche Stabilität. Eine fundierte Selbstanalyse hilft, Schnittstellen zu erkennen und Verantwortlichkeiten zu definieren.

   Zudem sollten sie ihre möglichen Beiträge in Form von Handlungen, Aufgaben oder Rollen zur Stärkung der Gesamtverteidigung identifizieren und definieren. Mithilfe einer Ist-Soll-Analyse können eigene Defizite erkannt werden. Diese Analyse sollte für verschiedene Szenarien erfolgen – Frieden, Krise, Krieg –, um resiliente Strukturen aufzubauen. Die Verantwortlichen dürfen ihr Wirken dabei nicht isoliert verstehen, denn alle Segmente beeinflussen sich gegenseitig.

2. **Netzwerk aufbauen & Schnittstellen analysieren**
   Leitfragen: Mit wem und wie arbeitet die eigene Organisation bzw. das eigene Unternehmen zusammen? Wer ist von dem Beitrag der eigenen Organisation betroffen?

   Die Zusammenarbeit zwischen den unterschiedlichen Beteiligten ist essenziell. Eine Schnittstellenanalyse hilft zu erkennen, mit wem sie sich abstimmen müssen – lokal, bundesweit und international. Ein frühzeitiger auch persönlicher Austausch bereits vor Eintritt einer Krise unterstützt die zeitgerechte Identifizierung von Schwachstellen und den Aufbau effektiver Kooperationsstrukturen. Regelmäßige gemeinsame Übungen sowie Austausch- und Abstimmungsformate inklusive Teilen von Erkenntnissen tragen dazu bei, Abläufe zu testen und zu optimieren. Denn: Ein ineffektives Zusammenspiel kann im Ernstfall zu Verzögerungen, Sicherheitsrisiken und erheblichem Schaden führen.

3. **Strategien und Lösungen entwickeln**
   Leitfrage: Welche gemeinsamen Lösungen und Maßnahmen können durch die eigene Organisation bzw. das eigene Unternehmen für die jeweiligen Beiträge entwickelt werden, um die Verteidigung zu stärken?

   Alle Beteiligten sollten ihre Rolle im Rahmen der Gesamtverteidigung definieren und eine Vision hierfür entwickeln. Basierend auf dieser Vision können messbare, realistische, relevante und zeitgebundene Ziele festgelegt werden. Hieraus sind konkrete Maßnahmen ableitbar, sie können priorisiert und in einen Umsetzungsplan überführt werden. Die handelnden Personen sollten diesen Prozess flexibel gestalten, um dynamische Entwicklungen berücksichtigen zu können. Maßnahmen sollten dabei auch nach Möglichkeit gemeinsam mit Partner:innen entwickelt werden, um Synergien zu nutzen und eine kohärente Verteidigungsstruktur zu etablieren. Für eine gute Vorbereitung sollten zudem verschiedene Szenarien sowie szenariospezifische Maßnahmen erarbeitet werden, um eine ganzheitliche Betrachtung und Vorbereitung auf unterschiedliche Situationen sicherzustellen.

4. **Kommunikation etablieren**
   Leitfrage: Wo reicht es aus, dass die eigene Organisation bzw. das eigene Unternehmen entsprechende Partner:innen nur informiert, und wo müssen Allianzen aufgebaut werden?

   Die entwickelten Strategien sollten alle Beteiligten sowohl intern als auch extern kommunizieren, um aufzuklären und Unterstützung zu sichern. Während einige Partner:innen lediglich informiert werden müssen, sind andere aktiv in die Umsetzung einzubinden. Regelmäßige Austauschformate, Workshops und Netzwerktreffen helfen, den erarbeiteten Umsetzungsplan umfassend zu verankern. Zudem sollten alle Beteiligten eine gezielte Öffentlichkeitsarbeit etablieren, um Transparenz über eigene Leistungen herzustellen, Berührungspunkte zur Bevölkerung darzustellen und auch die gesellschaftliche Akzeptanz für das Thema Gesamtverteidigung zu erhöhen.

5. **Adaption, Erprobung und Weiterentwicklung**
   Leitfrage: Wie kann sich die eigene Organisation bzw. das eigene Unternehmen stetig weiterentwickeln und an veränderte Rahmenbedingungen anpassen?

   Verteidigung ist ein dynamischer Prozess, der kontinuierliche Anpassungen erfordert. Alle zuvor genannten Schritte sollten die Akteur:innen regelmäßig wiederholen. Gleichzeitig ist das gemeinsame Üben notwendig, um Strategien und Abläufe zu testen sowie Schwachstellen zu identifizieren. Denn Veränderungen in der Bedrohungslage, technische Innovationen und geopolitische Entwicklungen erfordern eine flexible Anpassung von Maßnahmen. Wer Comprehensive Defence erfolgreich etablieren will, muss sich kontinuierlich weiterentwickeln.

   Die Integration von Comprehensive Defence ist eine langfristige Aufgabe, die alle Beteiligten fordert. Doch durch die systematische Vorgehensweise, eine strukturierte Analyse, Kooperation, strategische Planung, Kommunikation und fortlaufende Weiterentwicklung kann eine belastbare Sicherheitsstruktur geschaffen werden.

   Wer heute handelt, schafft die Grundlage für eine resiliente Gesellschaft und eine effektive gesamtstaatliche Verteidigung.

bwconsulting

Sicherheit muss heute als eine gesamtstaatliche und gesamtgesellschaftliche Aufgabe betrachtet werden, die eine umfassende und koordinierte Strategie erfordert – **genau hier setzt das Analyseframework Comprehensive Defence an.** Diese Broschüre ist die Zusammenfassung einer umfangreichen Studie. Für weitere Informationen steht unser Team gerne zur Verfügung.

Unser Team

Johannes Bader
Senior Manager

Leoni Lübbert
Senior Consultant

Kathrin Moog
Senior Consultant

Maurice Stette
Senior Consultant

Ralph Löhrer
Consultant

ComprehensiveDefence@bwconsulting.de

Bildnachweis:

Twardy/Bundeswehr
Hüttenhölscher/Bundeswehr
Weinrich/Bundeswehr
Fionn Große/Unsplash
alfa27/AdobeStock
Andrey Popov/AdobeStock
AnnaStills/AdobeStock
annanahabed/AdobeStock
AntonioDiaz/AdobeStock
Budimir Jevtic/AdobeStock
contrastwerkstatt/AdobeStock
deliris/AdobeStock
Drazen/AdobeStock
Dusan Petkovic/AdobeStock
fizkes/AdobeStock
Galina Zhigalova/AdobeStock
Gorodenkoff/AdobeStock
industrieblick/AdobeStock
insta_photos/AdobeStock
jackfrog/AdobeStock
kay fochtmann/AdobeStock
kerkezz/AdobeStock
KOTO/AdobeStock
Kzenon/AdobeStock
littlewolf1989/AdobeStock
Liubomir/AdobeStock
makedonski2015/AdobeStock
Martin Barraud/AdobeStock
Miljan Živković/AdobeStock
Miquel/AdobeStock
Monkey Business/AdobeStock
okrasiuk/AdobeStock
oksix/AdobeStock
peopleimages.com/CoetzeeRising/AdobeStock
peopleimages.com/K.A./AdobeStock
peopleimages.com/M Einero/AdobeStock
peopleimages.com/Nicholas Felix/AdobeStock
peopleimages.com/Siphosethu Fanti/AdobeStock
peopleimages.com/Sharne/AdobeStock
peopleimages.com/Tinashe Njaku/AdobeStock
Quality Stock Arts/AdobeStock
Rido/AdobeStock
Seventyfour/AdobeStock
Wellnhofer Designs/AdobeStock
Yakobchuk Olena/AdobeStock
zinkevych/AdobeStock

Die BwConsulting ist die Inhouse-Beratung der Bundeswehr.

Wir begleiten mit methodischer Expertise und fachlicher Kompetenz die strategischen Projekte des Bundesministeriums der Verteidigung (BMVg).

Ziel der BwConsulting ist es, Veränderungen zu ermöglichen und die nachhaltige Weiterentwicklung des gesamten Verteidigungsressorts zu fördern.

Das Unternehmen beschäftigt sich mit zukunftsweisenden Themen, die für die langfristige Widerstandsfähigkeit und den Erfolg der Bundeswehr entscheidend sind – wie Comprehensive Defence.

Als zentrale Partnerin für Innovation, Transformation und Gestaltung trägt die BwConsulting so aktiv zur Zukunftsfähigkeit der Bundeswehr und unserer Sicherheit bei.

Treten Sie mit uns in Kontakt

www.bwconsulting.de