Metis

Studie

Neue hybride Bedrohungen

Nr. 26 | Juli 2021

Institut für
Strategie & Vorausschau

Zusammenfassung

Hybride Kriege werden die internationale Sicherheitslage zukünftig noch stärker charakterisieren. In Friedenszeiten nutzen Staaten hybride Bedrohungen, um die Verwundbarkeit von komplexen und hochgradig vernetzten Gesellschaften auszunutzen und Kontrahenten durch einen permanenten »Scheinkriegszustand« zu schwächen. Es ist zu erwarten, dass hybride Bedrohungen zukünftig in weitere Gesellschaftsbereiche vordringen. Bestehende Sicherheitsarchitekturen müssen daher agiler werden, und Staaten wie die Bundesrepublik Deutschland müssen eine resiliente Sicherheitskultur aufbauen, um sich diesen Herausforderungen stellen zu können.

Eindeutig schwarze Chamäleons

Der Krieg ist ein Chamäleon. Er tritt in unterschiedlichsten Formen in Erscheinung. Seine Natur, bestehend aus der Triade Ziel (Niederwerfen des Gegners), Mittel (Anwendung physischer Gewalt) und politischer Zweck (Aufzwingen seines eigenen Willens), bleibt hingegen unverändert. Das primäre Verständnis von Krieg als einem konventionellen Konflikt zwischen Staaten ist eine besonders in der westlichen Welt etablierte Ansicht, die jedoch selbst einer kursorischen historischen Überprüfung nicht standhält. Obwohl schon das antike Kriegsverständnis die rechtlich geregelte, direkte Kriegsführung schwerer Infanterie auf einem festgelegten Schlachtfeld vorsah, vergifteten doch auch Griechen und Römer Brunnen, verbrannten Weideland oder nutzten Desinformation und Täuschung. Auch das Fundament der zeitgenössischen Ansätze *Western Way of War* (Präferenz zu direkter und präziser Kriegsführung mit hoher Opfersensibilität) oder *Democratic Warfighting* (Dominanz und Regelkonformität demokratischer gegenüber autokratischen Streitkräften) beschreibt nur idealtypische Kriegsformen, die in der Praxis selten ohne hybride Elemente auskommen. Klare Fronten, an denen Streitkräfte aufeinanderstoßen, Schonung der Zivilbevölkerung des Gegners, Restriktionen mit Blick auf die Formen und Mittel der militärischen Gewaltanwendung – in der Farbenlehre des Krieges sind derart konventionell geführten Konflikte schwarz und leicht vom Frieden in Weiß zu unterschieden. Die Grauzone wird dabei übersehen.

Die meisten Chamäleons sind grau

Diese idealtypische, »klassische« Lesart des Krieges trifft historisch lediglich auf eine kurze Phase der späten Neuzeit zu und beschränkt sich primär auf den europäisch geprägten geographischen Raum. Die historische Präferenz von Staaten zu direkter Kriegsführung liegt darin begründet, dass diese es erlaubt, eine Entscheidung auf Grundlage relativer Machtverteilung herbeizuführen. Solch ein Kriegsverständnis aber kann als Manifestation einer Vorliebe für staatszentrische Denkweise, die Konzentration auf strategische Schwerpunkte (Hauptstadt, Streitkräfte, Industriezentren) verstanden werden und ist somit Ausdruck einer dezidiert westlichen Perspektive. Konventionelle zwischenstaatliche Kriege sind auch zukünftig nicht auszuschließen, ihre Frequenz und Dauer nimmt aber seit 1945 stetig ab. Die Anzahl und Konfliktdauer asymmetrischer oder hybrider Kriege steigt demgegenüber kontinuierlich. Alle Zeichen deuten darauf hin, dass hybride Kriege zukünftig noch stärker dominieren werden. Besonderes Merkmal dieser Kriege ist eine Fluktuation der Konfliktintensität, eine Vermischung konventioneller und asymmetrischer Kriegsführung oder gar das ständige Unterschreiten eines echten Kriegszustands (politikwissenschaftlich definiert als 1000 Konfliktote pro Konfliktjahr). Aus »klassischer« – und nicht zuletzt auch aus völkerrechtlicher – Sicht schwelen diese Kriege in der Grauzone.

»Hybride Kriegsführung« ist dabei lediglich der neueste Vertreter einer jahrzehntelang geführten Begriffsdebatte,

mit der versucht wird, jene graustufigen Veränderungen des Krieges konzeptionell zu erfassen. Prominent wurde der Begriff im Zuge der Ukraine-Krise 2014. Vorab war er Teil der seit Mitte der 90er Jahre laufenden Debatte über Neue Kriege, *Low-Intensity Conflicts*[1], *Fourth-Generation Warfare*[2] oder asymmetrische Konflikte. All diese Konfliktdefinitionen teilen eine Gemeinsamkeit: Sie stellen Rationalisierungsansätze dar, die versuchen, jene modernen Kriegsformen zu erklären, die sich immer weiter vom westlich inspirierten Verständnis eines staatszentrischen, völkerrechtlich geregelten und konventionell geführten Kriegs entfernen. Empirisch untersucht werden in der Regel unkonventionelle Kriegsmittel, Guerillas, Aufstände, Völkermorde oder Terroranschläge sowie deren Kombination mit konventionellen Elementen. Ausgangspunkt bildet meist die quantitative Asymmetrie, also die Unterlegenheit einer Konfliktpartei im Sinne relativer Macht. Erst diese ist es, welche die unterlegene Seite dazu nötigt, von direkter Kriegsführung Abstand zu nehmen. Qualitative Asymmetrie ist die Kompensation der Unterlegenheit unter Nutzung konventioneller, aber insbesondere auch alternativer, terroristischer, irregulärer und krimineller Herangehensweisen. Sie ist das Herzstück asymmetrischer Kriegsführung. Es gilt, die eigenen Schwächen durch die Hervorhebung der eigenen Stärken zu kompensieren – und sich dabei vor allem die Schwächen des Gegners zu Nutze zu machen.

Von hybridem Krieg ist aktuell primär dann die Rede, wenn asymmetrische Kriegsführung abseits des Konfliktherds beziehungsweise der Front Anwendung findet. Ein Beispiel dafür könnte etwa das Abhören von Mobiltelefonen der Verwandten von Soldaten im Einsatz sein, um gefechtsnützliche Informationen abzugreifen. Alle erdenklichen Mittel, selbst solche, die auf den ersten Blick abstrus erscheinen, werden genutzt. Wenn solche hybriden Ansätze jenseits der klaren Konfliktlinien ihre Wirkung entfalten oder gänzlich ohne konventionellen Kriegszustand Anwendung finden, spricht man von hybriden Bedrohungen. Diese verursachen einen permanenten, latenten Zustand unterhalb der Kriegsschwelle. Ziel eines hybrid agierenden Akteurs ist die kontinuierliche Schwächung des Gegners, um die eigene Unterlegenheit auszubalancieren und seine Ausgangssituation in einem möglichen zukünftigen konventionellen Krieg zu verbessern. Zu diesem Zweck werden der gesellschaftliche Zusammenhalt, essenzielle öffentliche Güter, Infrastrukturen und Dienstleistungen, die Wirtschaftsordnung oder das öffentliche Meinungsbild Ziel von Subversion, Störung oder Unterminierung. Die Zivilbevölkerung eines Gegners wird dadurch zum primären strategischen Schwerpunkt. Hybride Bedrohungen generieren so unzählige Grautöne des Chamäleons Krieg, die es nahezu unmöglich machen, analytisch trennscharf einen echten Kriegszustand zu attestieren. Die durch den permanenten Scheinkriegszustand eintretende Schwächung, erzwungene Selbstbeschäftigung des Zielstaats, inklusive politischer, wirtschaftlicher und sozialer Lähmung, ermöglicht es dem Aggressor, entweder siegesgewiss konventionell zu eskalieren oder anderweitig global und ungestört, zu agieren.

Neue Grautöne durch Trendsetter Russland und China

Mit hybriden Bedrohungen verknüpft man vornehmlich die Aktivitäten der Russischen Föderation und Chinas, da diese Staaten in diesem Bereich sehr aktiv sind und in gewissem Maße als Trendsetter gelten können. Beide Staaten verfügen über beachtliche militärische Fähigkeiten, sind aber dennoch dem Westen unter Führung der USA konventionell unterlegen. Im Falle Russlands kommt eine relative ökonomische Schwäche hinzu. Zur Kompensation dieser Defizite und zur Wahrung der eigenen Handlungsfähigkeit erweiterte vornehmlich Russland asymmetrische Kriegsführung um die hybride Komponente. Vor allem der Ukraine-Konflikt verdeutlicht das Repertoire gängiger hybrider Ansätze. Dazu gehört zum Beispiel die Wahlbeeinflussung in westlichen Ländern, ökonomische Schwächung der Ukraine, die planmäßige Verbreitung von Fake News und Propaganda bis hin zu Cyberaktivitäten und Spionage gegen staatliche Einrichtungen in westlichen Staaten. Dieses breite Spektrum hybrider Bedrohungen Moskaus unterstützte die konventionelle Kriegsführung der bewusst ohne Insignien operierenden russischen Truppen in der Ost-Ukraine. Mit dem Abklingen der Konfliktintensität endete zwar der hybride Krieg; die hybriden Bedrohungen hingegen bleiben bestehen und wirken bis heute weiter gegen Europa, die USA und die Ukraine.

Abbildung 1 verdeutlicht das breite Anwendungsspektrum hybrider Ansätze. Was in Friedenszeiten mit hybriden Bedrohungen zur Demoralisierung und Destabilisierung des gesellschaftlichen Zusammenhalts und der politischen Stabilität beginnt, entwickelt sich hin zu indirekten Feindseligkeiten unter Anwendung wirtschaftlicher Zwangsmaßnahmen und Cyberangriffen.

Angriffe auf privatwirtschaftliche Akteure, um etwa kritische Infrastrukturen zu stören, Wirtschaftsspionage zu betreiben, wirtschaftlichen Schaden anzurichten oder die

1 Als »Neue Kriege« oder *Low-Intensity Conflicts* charakterisiert man Konflikte zwischen staatlichen und nicht-staatlichen Akteuren, die geprägt sind durch Kämpfe um Identitätspolitik im Gegensatz zur Ideologie, nicht-staatliche Finanzierung und Kämpfe um politische statt physischer Kontrolle von Territorium und Bevölkerung.

2 Während die ersten drei Generationen (Formationskriegsführung, Feuerkraft und Bewegungskrieg) zum Ziel hatten, die Streitkräfte eines Gegners physisch zu zerstören, zielt *Fourth-Generation Warfare* darauf ab, die psychische Fähigkeit eines Kontrahenten zur Kriegsführung zu überwinden, indem Entscheidungsträger durch öffentlichen Druck zu politischen Entscheidungen gezwungen werden.

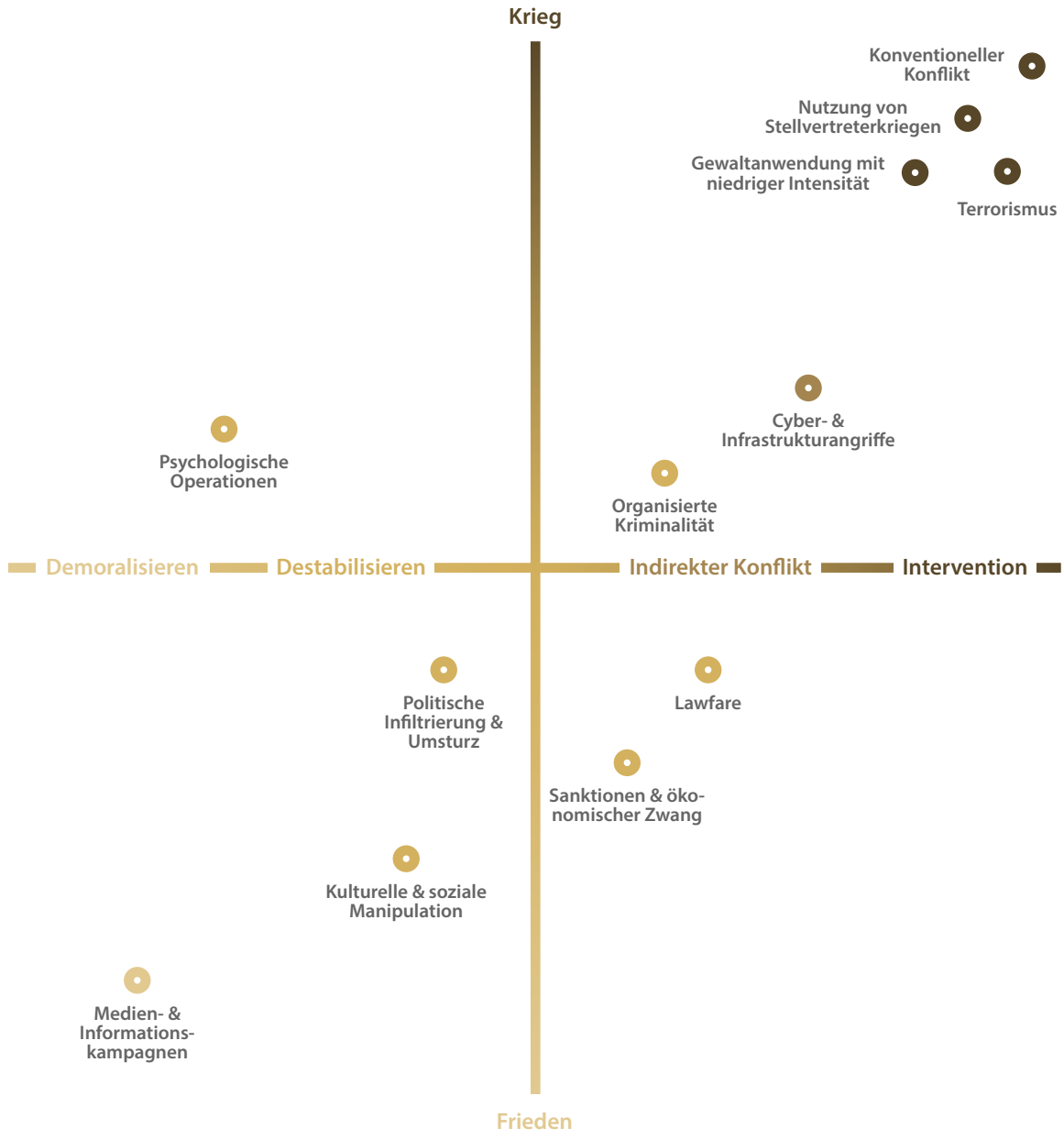


Abb. 1 ***Mittel hybrider Kriegsführung.*** | Quelle der Vorlage: https://cepa.org/lt-gen-ben-hodges-on-the-future-of-hybrid-warfare/

öffentliche Meinung zu beeinflussen wurden und werden weiter registriert und chinesischen oder russischen Gruppen vorgeworfen. Hinzu kommen subversivere Mittel, beispielsweise der Einsatz von Social Media Influencern und *Leaks*. Flankiert von staatlich finanzierten Medienanstalten werden so Parallelrealitäten, Gegennarrative und »alternative Wahrheiten« etabliert.

Bei einer Vielzahl hybrider Bedrohungen besteht zudem das Attributionsproblem: Initiator und Verursacher sind nicht eindeutig zu bestimmen, was es wiederum einfacher macht, Verantwortung von sich zu weisen. Russische Propaganda zielte bisher grundsätzlich immer zuerst auf die russische Minderheit in einem Zielland ab und entwickelt sich von dort dann weiter. Das folgt der Logik der *Fourth-Generation Warfare*, bei der nicht Kombattanten das Ziel militärisch organisierter Maßnahmen sind, sondern gesamte Gesellschaften samt ihren Entscheidungsträgern. Russland verfolgt mit dem Einsatz hybrider Maßnahmen somit das Ziel, eine strategische Wirkung zu erzielen, da es eine direkte Konfrontation mit der NATO nur schwer gewinnen und einen ökonomischen Wettlauf mit den USA oder der EU wohl eindeutig verlieren würde.

Abb. 2 ***»Einsamer Wolf« Hacker als hybride Bedrohung der Zukunft.*** | Quelle: https://www.shutterstock.com/g/shock

China hingegen nutzt hybride Maßnahmen – vor allem im Cyber-Bereich – um von eigenen strategischen Initiativen, wie beispielsweise der Schaffung künstlicher Inseln in der südchinesischen See oder der schleichenden Militarisierung wirtschaftlicher Stützpunkte entlang der Seidenstraßen, abzulenken.

Hybride Bedrohungen und die graue Zukunft

Neben den bereits bekannten Erscheinungsformen hybrider Bedrohungen müssen sich westliche Staaten auf eine Vielzahl neuer Angriffsarten und die Ausnutzung neuer Schwachpunkte vorbereiten. Es wird nicht ausreichen, die Erfahrungen und Erkenntnisse der Ukraine-Krise von 2014 einfach in die Zukunft zu extrapolieren. Mögliche zukünftige hybride Bedrohungen sind vor allem im rechtlichen Raum, im Finanz- sowie im Kommunikationssektor zu erwarten. Viele der zukünftigen hybriden Bedrohungen werden nicht grundlegend neu sein und bereits bekannte Ansätze häufig nur erweitern. Neu wird allerdings die Qualität dieser hybriden Angriffe ebenso wie ihr zeitkritischer Einsatz, was die Reaktionsfähigkeit betroffener Staaten überfordern kann. Der folgende Abschnitt skizziert vorausschauend mögliche Zukunftsfelder hybrider Bedrohungen, weit unterhalb der Schwelle hybrider Kriege.

Bots mit künstlicher Intelligenz (KI)

Im Bereich der KI eröffnen zukünftige technische Möglichkeiten neue Handlungsspielräume.[3] Die Fähigkeiten von Bots zur Beeinflussung der öffentlichen Meinung werden damit drastisch zunehmen. Menschenähnlich wirkende KI-Bots werden authentischer und kaum von echten im Netz anzutreffenden Individuen zu unterscheiden sein. KI-Bot Personas werden automatisch generierte Artikel zu politischen, gesellschaftlichen oder wirtschaftlichen Themen verfassen. Gepaart mit authentisch wirkenden *Deepfake* Video- und Audioinhalten werden sie millionenfach in Diskurse einsteigen und diese beeinflussen. Meinungsbildung in pluralistischen Demokratien kann dadurch zielgerichteter denn je von außen manipuliert werden. Derzeit lassen sich die meisten computergenerierten Textinhalte, Kommentare, Bilder oder Videos noch vergleichsweise leicht als Fakes enttarnen. In naher Zukunft wird sowohl die Fülle als auch die gesteigerte Qualität spezielle forensische Methoden notwendig machen.

Blitzattacken im Finanzsektor

Hybride Bedrohungen im Finanzsektor existieren bereits in Form von feindlichen Firmenübernahmen, Patentübertragungen, Wirtschaftsspionage, Cyberangriffen auf Börsen oder gezielte Marktmanipulation. Ziel ist es meist, einen finanziellen Ausnahmezustand oder politischen Druck zu generieren, um die Handlungsfähigkeit des Angegriffenen einzuschränken und Regierungen zu bestimmten Handlungen wie beispielsweise Konzessionen, Subventionen, Hilfskrediten oder dem Deklarieren regulatorischer Freiräume zu bewegen. Auch die gezielte Abwerbung von Schlüsselpersonal durch Geheimdienste entfaltet wirtschaftliches Schadenspotenzial. Neue Vulnerabilitäten im Finanzsektor sind im Zuge dezentralisierter Finanzplätze zu erwarten. Gepaart mit staatlichen Anstrengungen, digitale – wenn auch zentralisierte – Blockchain-Ableger des Euro, Dollar oder Yuan zu etablieren, wird sich zukünftig die Angriffsfläche vergrößern. Ein aktuelles Beispiel findet sich im Arbitrage-Handel, also der Ausnutzung von Kurs-, Zins- oder Preisunterschieden von Aktien und Währungen auf unterschiedlichen Börsen. Während klassische Marktmanipulation durch koordiniertes Vorgehen mehrerer Marktteilnehmer oder durch Insiderhandel gekennzeichnet ist, sind im digitalen Raum sogenannte *Flash-Loan*-Angriffe in Mode: Anonyme Händler leihen sich für einige Sekunden Millionen oder Milliarden Dollar, kaufen sich auf einer Börse einen Titel und fluten damit eine weitere Börse bis Kurse ins Bodenlose sinken. Solche *Flash-Loan*-Transaktionen dauern nur wenige Sekunden und können Milliardenschäden verursachen, einzelne Firmen (zum Beispiel solche mit militärischen Schlüsseltechnologien) vom Markt fegen, Volkswirtschaften lähmen oder Währungen destabilisieren. Wofür klassische Mittel der ökonomischen Zwangsausübung, wie Sanktionen, Jahre brauchten, sind zukünftig wenige, kurze, zerstörerische Schläge möglich.

Auslösen von Umweltkatastrophen

Die Effekte des Klimawandels generieren neue ökologische Vulnerabilitäten, die zukünftig Zielscheibe für hybride Bedrohungen werden können. Gezielte und gleichzeitige Brandstiftung in dutzenden Waldgebieten wären ein mögliches Mittel zur Überlastung und Destabilisierung staatlicher Sicherheits- und Krisenmanagementorgane. Auch Cyberattacken auf kritische Infrastrukturen, die ökologische Folgekatastrophen nach sich ziehen, sind denkbar. Fokussiert sich ein Staat und dessen Gesellschaft auf die Bewältigung von Naturkatastrophen ist er meist stark ausgelastet oder gar paralysiert. Außenpolitische Entwicklungen werden dann zumindest in der öffentlichen Wahrnehmung zweitrangig und erschweren den Entscheidungsfindungsprozess aufgrund dringlicherer nationaler Krisen.

Lawfare

Die Ausnutzung realer, vermeintlicher oder sogar inszenierter Vorfälle von Kriegsvölkerrechtsverletzungen, die bereits heute als unkonventionelles Mittel zur Konfrontation einer überlegenen Militärmacht eingesetzt werden, können die globale öffentliche Meinung mobilisieren. Das »Recht als Waffe« zielt also auf die Manipulation des

3 Siehe „Quantentechnologie: Implikationen für Sicherheit und Verteidigung", Metis Studie Nr. 25 (Mai 2021).

Völkerrechtsdiskurses, auf Alternativauslegungen oder auf die Nutzung einseitiger nationaler Gesetzgebung, die die eigene Interpretation internationaler Normen und Regeln stützt. Zukünftig werden hybride Akteure auch vor nationalen Gerichten rechtliche Verfahren und die Ausnutzung des Rechtsweges für ihre Zwecke nutzen. *Lawfare* gegen nationale Rechtssysteme zielt einerseits auf Überlastung. Durch die Ausschöpfung rechtlicher Verfahren bis in die letzte Instanz in nicht zu bewältigender Fülle, werden die betroffenen Institutionen durch Überflutung gelähmt und Verfahren um Jahre verlängert. Andererseits werden konkurrierende Rechtsauslegungen in verschiedenen Ländern eingeholt, um eine wechselseitige Delegitimation zu erreichen.

Handlungsempfehlungen

Westliche Demokratien sind aufgrund ihrer gesellschaftlichen Offenheit, ihrer hochgradigen technischen Vernetzung und privatwirtschaftlichen Ausrichtung sehr verwundbar gegenüber aktuellen und zukünftigen hybriden Bedrohungen. Presse- und Meinungsfreiheit lässt die Verbreitung von Desinformation zu; der gesellschaftliche Vernetzungsgrad erhöht das Risiko von Kettenreaktionen; die Privatwirtschaft bereitet sich mit einem unkoordinierten Flickenteppich aus Maßnahmen auf mögliche hybride Risiken vor.

Gleichzeitig sind Demokratien auch lernfähiger, innovativer und resilienter als andere Staatsformen. Wenn sie ihr staatszentrisches Denken in Teilen ablegen, können sie sich auf neue Herausforderungen einstellen. Um der Ganzheitlichkeit des hybriden Vorgehens Russlands und Chinas auch in Zukunft entgegenwirken zu können, sollten folgende Handlungsempfehlungen, mit dem Ziel die Absorptionsfähigkeit und Resilienz zu steigern [4], in Betracht gezogen werden:

Investitionen in Resilienzmechnismen tätigen

- Minimalstandards für Cybersicherheit gesetzlich fixieren und technologischen Entwicklungen stets anpassen
- Widerstands- und Reaktionsfähigkeit staatlicher Institutionen durch Entbürokratisierung neuralgischer Verfahren steigern
- Verfahren zur Abkopplung kritischer Infrastrukturen etablieren und Redundanzen schaffen, um im Krisenfall Kettenreaktionen einzudämmen

Frühwarnung etablieren

- Ressortgemeinsames Frühwarnsystem zur Erkennung von organisierter Desinformation
- Früherkennungsfähigkeiten privater Akteure aus Industrie-, Energie-, IT-Sektor in gesamtstaatliches Frühwarnsystem integrieren
- Informationsaustausch auf nationaler Ebene subsidiär aufbauen

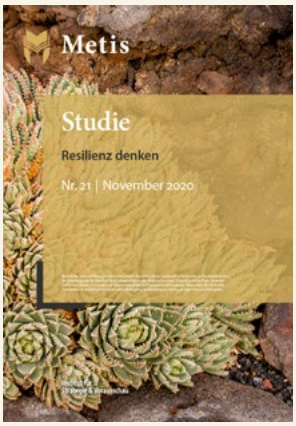
Resilienz steigern

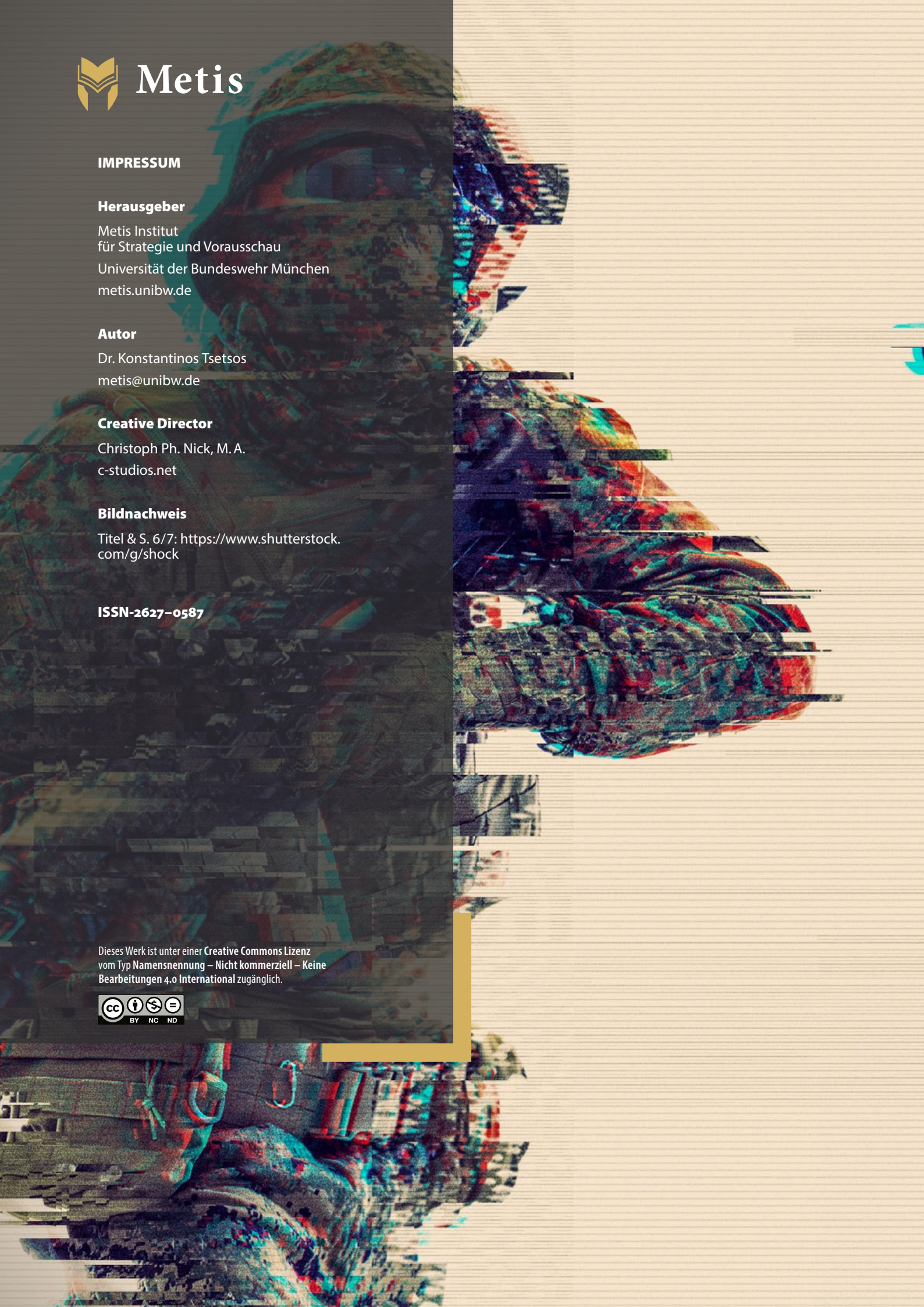
- Nationales Krisenreaktions- und Krisenmanagementsystem etablieren und dieses an EU- und NATO-Institutionen für die multinationale Koordination anknüpfen
- zivil-militärische Zusammenarbeit über reaktive Amtshilfe hinaus hin zu proaktiver Prävention ausbauen und private Akteure inkludieren
- Kooperation zwischen staatlichen, öffentlichen und vor allem privaten Akteuren forcieren und Gegen- und Sicherungsmaßnahmen koordinieren
- subsidiäre Koordination- und Resilienzmechanismen etablieren, die beim Landkreis beginnend über Mitgliedsstaat bis zur EU und NATO reichen
- strategische Kommunikation hinsichtlich hybrider Bedrohungen gegenüber der Bevölkerung intensivieren, um diese stärker zu sensibilisieren
- Sicherheitskultur durch Aufmerksamkeits-, Aufklärungs- und Informationskampagnen etablieren
- Gegenmaßnahmen sollten einem vernetzten, gesamtstaatlichen und ressortübergreifenden Ansatz folgen (*Whole of Governement Approach*); gesamtstaatliche Aktivitäten müssen aber durch die Inklusion privater Akteure augmentiert werden, um das Ziel gesamtgesellschaftlicher Resilienz zu erreichen (*Whole of Nation Approach*)
- die Vertiefung der Kooperation zwischen staatlichem und privatem Sektor sollte über symbolische Deklarationen hinausgehen; für private Unternehmen sind gesetzliche Vorgaben und Anreize zu schaffen, die eine enge Kooperation, ohne wirtschaftliche Nachteile, mit staatlichen Institutionen erlauben

4 Siehe „Resilienz denken", Metis Studie Nr. 21 (November 2020).

Metis Publikationen

Bisher ebenfalls erschienen und zu finden auf der Metis Website unter metis.unibw.de





Metis

IMPRESSUM

Herausgeber

Metis Institut
für Strategie und Vorausschau
Universität der Bundeswehr München
metis.unibw.de

Autor

Dr. Konstantinos Tsetsos
metis@unibw.de

Creative Director

Christoph Ph. Nick, M. A.
c-studios.net

Bildnachweis

Titel & S. 6/7: https://www.shutterstock.com/g/shock

ISSN-2627–0587